Política de Certificado de Assinatura Digital Tipo A1 da Autoridade Certificadora de Defesa (AC Defesa)

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

Infraestrutura de Chaves Públicas Brasileira ICP-Brasil

Sumário

CONTROLE DE VERSÃO

VERSÃO	DATA	DESCRIÇÃO
1.0	24/04/2017	Versão inicial, a partir do DOC-ICP-04 versão 6.0
1.1	15/09/2017	Alterações conforme DOC-ICP-04 versão 6.3
1.2	01/02/2019	Alterações conforme DOC-ICP-04 versão 6.7

TABELA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CG	Comitê Gestor
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CMVP	Cryptographic Module Validation Program
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COBIT	Control Objectives for Information and related Technology
COSO	Comitee of Sponsoring Organizations
CPF	Cadastro de Pessoas Físicas
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
ICP-Brasil	Infraestrutura de Chaves Pública Brasileira
IDS	Sistemas de Detecção de Intrusão
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	National Institute of Standards and Technology
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
OU	Organization Unit

SIGLA	DESCRIÇÃO
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	Proof of Possession
PSS	Prestadores de Serviço de Suporte
RFC	Request for Comments
RG	Registro Geral
SGC	Sistema de Gerenciamento de Certificado
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
TCSEC	Trusted System Evaluation Criteria
TSDM	Trusted Software Development Methodology
UF	Unidade da Federação
URL	Uniform Resource Location

1 INTRODUÇÃO

1.1 VISÃO GERAL

1.1.1 Esta política tem por finalidade estabelecer os procedimentos de certificação e as características do Certificado de Assinatura Digital Tipo A1 da Autoridade Certificadora de Defesa (AC Defesa) na Infraestrutura de Chaves Públicas Brasileira.

1.1.2 A estrutura desta política está baseada no DOC-ICP-04 do Comitê Gestor da ICP-Brasil - Requisitos Mínimos para as Políticas de Certificados na ICP-Brasil e na RFC 3647 (*Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework*).

1.2 IDENTIFICAÇÃO

1.2.1 Esta PC é chamada "Política de Certificado de Assinatura Digital Tipo A1 da Autoridade Certificadora de Defesa (AC Defesa)" e referida como "PC A1 da AC Defesa". Esta PC descreve os usos relacionados ao certificado de Assinatura Digital correspondente ao tipo A1 do DOC-ICP-04 do Comitê Gestor da ICP-Brasil. O OID (*object identifier*) desta PC é 2.16.76.1.2.1.78.

1.3 COMUNIDADE E APLICABILIDADE

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 Os dados a seguir, referentes à Autoridade de Registro (AR) utilizada pela AC Defesa para os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são publicados na página web da AC Defesa *http://www.acdefesa.mil.br*:

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

b) para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar;

c) para cada AR credenciada, relação de postos de validação remotos, autorizados pela AC Raiz a funcionar, seus respectivos endereços e dados de seus responsáveis;

d) para cada AR credenciada, relação de eventuais postos provisórios autorizados pela AC Raiz a funcionar, com data de criação e encerramento de atividades;

e) relação de AR que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento;

f) relação de instalações técnicas de AR credenciadas que tenham deixado de operar, com respectiva data de encerramento das atividades;

g) acordos operacionais celebrados pelas AR vinculadas com outras AR da ICP-Brasil, se for o caso.

1.3.2.2 A AC Defesa mantém as informações acima atualizadas.

1.3.3 Prestador de Serviço de Suporte

1.3.3.1 A relação de todos os Prestadores de Serviço de Suporte - PSS vinculados diretamente a AC Defesa ou por intermédio de suas AR é publicada na página web da AC Defesa *http://www.acdefesa.mil.br*.

1.3.3.2 PSS são entidades utilizadas pela AC e suas AR para desempenhar atividade descrita nesta PC e se classificam em três categorias, conforme o tipo de atividade prestada:

a) disponibilizar infraestrutura física e lógica;

b) disponibilizar recursos humanos especializados; ou

c) disponibilizar infraestrutura física e lógica e de recursos humanos especializados.

1.3.3.3 A AC Defesa mantém as informações acima atualizadas.

1.3.4 Titulares de 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.

1.3.5 Aplicabilidade

1.3.5.1 Esses certificados se destinam exclusivamente à utilização em assinatura digital, não repúdio, garantia de integridade de informação e autenticação de seu titular.

1.3.5.2 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.

1.3.5.3 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 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.

1.3.5.4 Os certificados emitidos pela AC Defesa no âmbito desta PC podem ser utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.3.5.5 Não se aplica.

1.3.5.6 Não se aplica.

1.3.5.7 Não se aplica.

1.3.5.8 Não se aplica.

1.4 DADOS DE CONTATO

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

2 DISPOSIÇÕES GERAIS

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

2.1 OBRIGAÇÕES E DIREITOS

2.1.1 Obrigações da AC Defesa

2.1.2 Obrigações da AR

2.1.3 Obrigações do Titular do Certificado

2.1.4 Direitos da Terceira Parte (*Relying Party*)

2.1.5 Obrigações do Repositório

2.2 RESPONSABILIDADES

3.1.11 Autenticação da Identidade de um equipamento ou uma aplicação

3.1.11.1 Disposições Gerais

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

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

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

3.3 GERAÇÃO DE NOVO PAR DE CHAVES APÓS EXPIRAÇÃO OU REVOGAÇÃO

3.4 SOLICITAÇÃO DE REVOGAÇÃO

4 REQUISITOS OPERACIONAIS

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

4.1 SOLICITAÇÃO DE CERTIFICADO

4.2 EMISSÃO DE CERTIFICADO

4.3 ACEITAÇÃO DE CERTIFICADO

4.4 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.4.1 Circunstâncias para revogação

4.4.2 Quem pode solicitar revogação

4.4.3 Procedimento para solicitação de revogação

4.4.4 Prazo para solicitação de revogação

4.4.5 Circunstâncias para suspensão

4.4.6 Quem pode solicitar suspensão

4.4.7 Procedimento para solicitação de suspensão

4.4.8 Limites no período de suspensão

4.8 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

4.8.1 Recursos computacionais, software e dados corrompidos

4.8.2 Certificado de entidade é revogado

4.8.3 Chave de entidade é comprometida

4.8.4 Segurança dos recursos após desastre natural ou de outra natureza

4.8.5 Atividades das Autoridades de Registro

4.9 EXTINÇÃO DOS SERVIÇOS DA AC, AR OU PSS

5 CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

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

5.1 CONTROLE FÍSICO

5.1.1 Construção e localização das instalações de AC

5.1.2 Acesso físico nas instalações de AC

5.1.2.1 Sistema de Controle de Acesso

5.1.2.2 Mecanismos de emergência

5.1.3 Energia e ar-condicionado nas instalações da AC

5.1.4 Exposição à água nas instalações da AC

5.1.5 Prevenção e proteção contra incêndio nas instalações da AC

5.1.6 Armazenamento de mídia nas instalações da AC

5.1.7 Destruição de lixo nas instalações da AC

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

5.1.9 Instalações técnicas de AR

5.2 CONTROLES PROCEDIMENTAIS

5.2.1 Perfis qualificados

5.2.2 Número de pessoas necessário por tarefa

5.2.3 Identificação e autenticação para cada perfil

5.3 CONTROLES DE PESSOAL

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

5.3.2 Procedimentos de Verificação de Antecedentes

5.3.3 Requisitos de treinamento

5.3.4 Frequência e requisitos para reciclagem técnica

5.3.5 Frequência e sequência de rodízios de cargos

5.3.6 Sanções para ações não autorizadas

5.3.7 Requisitos para designação de pessoal

5.3.8 Documentação fornecida ao pessoal

6 CONTROLES TÉCNICOS DE SEGURANÇA

6.1 GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

6.1.1 Geração do Par de Chaves

6.1.1.1 O par de chaves criptográficas é gerado pelo titular do certificado, quando este for uma pessoa física e gerado pela pessoa responsável, indicada por seu(s) representante(s) legal(is), quando for uma pessoa jurídica.

6.1.1.2 A geração do par de chaves criptográficas ocorre, no mínimo, utilizando CSP (*Cryptographic Service Provider*) existente na estação do solicitante. Quando da geração, a chave privada é armazenada no HD da estação. A chave privada poderá ser exportada e armazenada (cópia de segurança) em mídia externa (*pen-drive*, *token* ou cartão inteligente) e protegida por senha de acesso.

6.1.1.3 O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados 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 do titular do certificado deve ser gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1]. As chaves privadas correspondentes aos certificados poderão ser armazenadas em repositório protegido por senha, cifrado por software no meio de armazenamento definido para o tipo de certificado A1.

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

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

a) a chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;

b) a chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida e deve estar protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;

c) a chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

6.1.1.7 O meio de armazenamento não deve modificar os dados a serem assinados, nem impedir que estes dados sejam apresentados ao signatário antes do processo de assinatura. O tipo de certificado emitido pela AC Defesa e descrito nesta PC é o A1.

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

6.1.1.8 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

Item não aplicável.

6.1.3 Entrega da chave pública para emissor de certificado

A entrega da chave pública do solicitante do certificado AC Defesa, é feita por meio eletrônico, em formato PKCS#10, por intermédio de uma sessão segura *SSL*.

6.1.4 Disponibilização de chave pública da AC para usuários

A AC Defesa disponibiliza o seu certificado, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, por intermédio de endereço *web*: *http://www.acdefesa.mil.br*.

6.1.5 Tamanhos de chave

6.1.5.1 O tamanho das chaves criptográficas associadas aos certificados Tipo A1 emitidos pela AC Defesa é de **2048 bits.**

6.1.5.2 Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo A1 da ICP-Brasil estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [1].

6.1.6 Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas dos titulares de certificados adotam, no mínimo, o padrão FIPS (*Federal Information Processing Standards*) 140-2 ou equivalente estabelecido pelo CG da ICP-Brasil.

6.1.7 Verificação da qualidade dos parâmetros

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

6.1.8 Geração de chave por *hardware* ou *software*

A geração das chaves criptográficas do Certificado Tipo A1 desta PC é realizada por *software*.

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

Os certificados têm ativados os bits ***digitalSignature***, ***nonRepudiation*** e ***keyEncipherment***.

6.2 PROTEÇÃO DA CHAVE PRIVADA

6.2.1 Padrões para software criptográfico

Os Titulares de Certificados devem garantir que os padrões, definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1], são observados para geração das chaves criptográficas.

6.2.2 Controle "n" de "m" para chave privada

Não se aplica.

6.2.3 Recuperação *(escrow)* de chave privada

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

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

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

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

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

6.2.4.4 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 assinatura digital 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 software criptográfico

Os Titulares de Certificados poderão optar por utilizar um hardware criptográfico sem capacidade de geração de chave, cartão inteligente ou token, para armazenar sua chave privada após a aceitação do certificado.

6.2.7 Método de ativação de chave privada

O titular do certificado pode definir procedimentos necessários para a ativação de sua chave privada.

6.2.8 Método de desativação de chave privada

O titular de certificado pode definir procedimentos necessários para a desativação de sua chave privada.

6.2.9 Método de destruição de chave privada

O titular de certificado pode definir procedimentos necessários para a destruição de sua chave privada.

6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1 Arquivamento de chave pública

As chaves públicas dos titulares de certificados de assinatura digital emitidos pela AC Defesa permanecem armazenadas após a expiração dos certificados correspondentes, permanentemente, na forma da legislação em vigor, para verificação de assinaturas geradas durante seu período de validade.

6.3.2 Períodos de uso para as chaves pública e privada

6.3.2.1 As chaves privadas de assinatura 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 assinaturas 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 Assinatura Digital Tipo A1 da AC Defesa é de **1 ano**.

6.4 DADOS DE ATIVAÇÃO

6.4.1 Geração e instalação dos dados de ativação

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

6.4.2 Proteção dos dados de ativação

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

6.4.3 Outros aspectos dos dados de ativação

Não se aplica.

6.5 CONTROLES DE SEGURANÇA COMPUTACIONAL

6.5.1 Requisitos técnicos específicos de segurança computacional

O titular do certificado é responsável pela segurança computacional dos sistemas nos quais são geradas e utilizadas as chaves privadas e deve zelar por sua integridade. O equipamento onde são gerados os pares de chaves criptográficas do titular do Certificado deve dispor de mecanismos mínimos que garantam a segurança computacional, com proteção antivírus e criptografia para a chave privada armazenada no HD.

6.5.2 Classificação da segurança computacional

Item descrito na DPC AC Defesa em vigor.

6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1 Controles de desenvolvimento de sistema

Item descrito na DPC AC Defesa em vigor.

6.6.2 Controles de gerenciamento de segurança

Item descrito na DPC AC Defesa em vigor.

6.6.3 Classificações de segurança de ciclo de vida

Não se aplica.

6.7 CONTROLES DE SEGURANÇA DE REDE

Item descrito na DPC AC Defesa em vigor.

6.8 CONTROLES DE ENGENHARIA DO SOFTWARE CRIPTOGRÁFICO

Os Titulares de Certificado devem garantir que o software criptográfico utilizado na geração e utilização de suas chaves criptográficas seguem os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

7 PERFIS DE CERTIFICADO E LCR

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

7.1 PERFIL DO CERTIFICADO

Todos os certificados emitidos pela 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

Os certificados emitidos pela AC Defesa implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2 Extensões de certificado

7.1.2.1 Neste item, a PC descreve todas as extensões de certificado utilizadas e sua criticalidade.

7.1.2.2 Extensões Obrigatórias

Os certificados emitidos pela AC Defesa obedecem a ICP-Brasil, que define como obrigatórias as seguintes extensões:

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

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

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

1) o campo *policyIdentifier* contém o OID desta PC: 2.16.76.1.2.1.78;

2) o campo *policyQualifiers* contém o endereço Web da DPC AC Defesa que emite o certificado: *http://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) *http://repositorio-acp.acdefesa.mil.br/lcr/acdefesa-v0.crl*;

2) *http://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-caIssuer, utilizando o protocolo de acesso HTTP, para a recuperação da cadeia de certificação no seguinte endereço:

1) *http://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*", definida como obrigatória pela ICP-Brasil, não crítica e com os seguintes formatos:

a) Para certificado de pessoa física:

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

1.1) **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;

1.2) **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;

1.3) **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.

2) 1 (um) campo *otherName*, não obrigatório, contendo:
rfc822Name, contém o endereço e-mail do titular do certificado;

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.

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.

b) Para certificado de pessoa jurídica:

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

1.1) **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;

1.2) **OID = 2.16.76.1.3.2 e conteúdo =** nome do responsável pelo certificado;

1.3) **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;

1.4) **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.

2) 1 (um) campo *otherName*, não obrigatório, contendo:
rfc822Name, contém o endereço e-mail do responsável pelo certificado.

7.1.2.4 Os campos *otherName*, definidos como obrigatórios, estão de acordo com as seguintes especificações:

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

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

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

d) Todas as informações de tamanho variável, referentes a números, tal como RG, são preenchidos com caracteres "zero" a sua esquerda para que seja completado seu máximo tamanho possível;

e) As 10 (dez) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, sendo utilizados apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre municípios e UF do Título de Eleitor;

f) 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.

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

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

A AC Defesa implementa a extensão "*Extended Key Usage*", não crítica, contendo os seguintes valores:

a) "*clientAuthentication*" (OID 1.3.6.1.5.5.7.3.2);

b) "*emailProtection*" (OID 1.3.6.1.5.5.7.3.4).

7.1.2.7 Não se aplica.

7.1.3 Identificadores de algoritmo

Os certificados emitidos pela AC Defesa 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

O nome do titular do certificado, constante do campo "*Subject*", adota o "*Distinguished Name*" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:
C = BR
O = ICP-Brasil
OU = Autoridade Certificadora de Defesa
OU = CNPJ da AR DEFESA
OU = Certificado PF A1 (no caso de certificado de pessoa física)
OU = Certificado PJ A1 (no caso de certificado de pessoa jurídica)
CN = nome do titular do certificado:CPF (no caso de certificado de pessoa física)
CN = razão social:CNPJ (no caso de certificado de pessoa jurídica)
Será escrito o nome até o limite do tamanho do campo disponível, vedada a abreviatura.

7.1.5 Restrições de nome

7.1.5.1 As restrições aplicáveis para os nomes dos titulares de certificado emitidos pela AC Defesa são as seguintes:

- não são admitidos sinais de acentuação, trema ou cedilhas;

- apenas são admitidos sinais alfanuméricos e os caracteres especiais descritos na tabela abaixo:

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

7.1.6 OID (Object Identifier) de Política de Certificado

O OID desta PC é: 2.16.76.1.2.1.78. Todo certificado emitido segundo essa PC, PC A1 AC Defesa, contém o valor desse OID presente na extensão *Certificate Policies*.

7.1.7 Uso da extensão "*Policy Constraints*"

Item não aplicável.

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 *http://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(s) 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 da AC Defesa 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;

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

8 ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1 PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO

Alterações nesta PC podem ser realizadas pela AC Defesa. A aprovação e consequente adoção de nova versão estarão sujeitas à autorização da AC Raiz.

8.2 POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO

A AC Defesa mantém página específica com a versão corrente desta PC para consulta pública, a qual está disponibilizada no endereço *web: http://www.acdefesa.mil.br*.

8.3 PROCEDIMENTOS DE APROVAÇÃO

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 PRO-

CEDIMENTOS 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.

9 DOCUMENTOS REFERENCIADOS

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

Ref.	Nome do documento	Código
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03

9.2 Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sitio *http://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
[2]	ATRIBUIÇÃO DE OID NA ICP-BRASIL	DOC-ICP-04.01

9.3 Os documentos abaixo são aprovados pela AC Raiz, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio *htt p://www.iti.gov.br*.

Ref.	Nome do documento	Código
[4]	MODELO DE TERMO DE TITULARIDADE	ADE-ICP-05.A
[5]	MODELO DE TERMO DE RESPONSABILIDADE	ADE-ICP-05.B