www.serpro.gov.br

Política de Certificado
da
Autoridade Certificadora
do
SERPROACF SSL A1

Autenticação de Servidor (SSL/TLS)

(PC ACSERPROACF SSL A1)

Versão 1.1 de Janeiro 2017

Serviço Federal de Processamento de Dados SERPRO

SUMÁRIO

TABELA DE SIGLAS

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	Comitê Gestor
CMM-SEI	*Capability Maturity Model* do *Software Engineering Institute*
CMVP	*Cryptographic Module Validation Program*
CN	*Common Name*
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COBIT	*Control Objectives for Information and related Technology*
COSO	*Comitee of Sponsoring Organizations*
CPF	Cadastro de Pessoas Físicas
DMZ	Zona Desmilitarizada
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	*Intrusion Detection System*
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
ITSEC	*European Information Technology Security Evaluation Criteria*
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	*National Institute of Standards and Technology*
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
OU	*Organization Unit*
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	*Proof of Possession*
PS	Política de Segurança
PSS	Prestadores de Serviço de Suporte
RFC	*Request For Comments*
RG	Registro Geral
SNMP	*Simple Network Management Protocol*
TCSEC	*Trusted System Evaluation Criteria*
TSDM	*Trusted Software Development Methodology*
UF	Unidade de Federação
URL	*Uniform Resource Locator*

1. INTRODUÇÃO

1.1. VISÃO GERAL

1.1.1 Este documento estabelece os requisitos a serem obrigatoriamente observados pelas SERPROACF SSL integrante da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de suas Políticas de Certificado - PC.

1.1.2 A PC SERPROACF 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 O tipo de certificado emitido sob esta PC é o certificado de assinatura do Tipo A1.

1.1.4 Os tipos de certificados de A1 a A4 e de S1 a S4, definem escalas de requisitos de segurança, nas quais os tipos A1 e S1 estão associados aos requisitos menos rigorosos e os tipos A4 e S4 aos requisitos mais rigorosos.

1.1.5 Certificados dos tipos de A1 a A4 e de S1 a S4, de assinatura ou de sigilo, podem, conforme a necessidade, ser emitidos pelas ACs para pessoas físicas, pessoas jurídicas, equipamentos ou aplicações.

1.1.6 Item não aplicável.

1.1.7 Outros tipos de certificado podem ser propostos para a apreciação do Comitê Gestor da ICP-Brasil – CG da ICP-Brasil. As propostas serão analisadas quanto à conformidade com as normas específicas da ICP-Brasil e, quando aprovadas, serão acrescidas aos tipos de certificados aceitos pela ICP-Brasil.

1.2. IDENTIFICAÇÃO

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

1.2.2 Após o processo de credenciamento da SERPROACF SSL foi atribuído a esta Política de Certificação, no âmbito da ICP-Brasil, o seguinte OID;

TIPO DE CERTIFICADO	OID
A1	2.16.76.1.2.1.89

1.3. COMUNIDADE E APLICABILIDADE

1.3.1. Autoridades Certificadoras

1.3.1.1 A Autoridade Certificadora do SERPRO Final SSL (ACSERPROACF SSL) integra a Infra-estrutura de Chaves Públicas Brasileira, ICP-Brasil, sob a hierarquia da Autoridade Certificadora do SERPRO (ACSERPRO) e da Autoridade Certificadora Raiz Brasileira.

1.3.1.2 Esta PC é implementada pela Autoridade Certificadora SERPROACF SSL cuja DPC (DPC ACSERPROACF SSL) encontra-se publicada em sua página *Web* no seguinte endereço: *https://certificados.serpro.gov.br/acserproacfssl.*

1.3.2. Autoridades de Registro

1.3.2.1 O endereço da página web (URL) da ACSERPROACF SSL é *https://certificados.serpro.gov.br/acserproacfssl* onde estão publicados os dados abaixo referentes as Autoridades de Registro, responsáveis pelos processos de recebimento, validação 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) para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar;
c) para cada AR credenciada, relação de eventuais postos provisórios autorizados pela AC Raiz a funcionar, com data de criação e encerramento de atividades;
d) relação de AR que tenham sido descredenciadas da cadeia da AC, com a respectiva data do descredenciamento;
e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectiva data de encerramento das atividades;
f) acordos operacionais celebrados pelas AR vinculadas com outras AR da ICP-Brasil, se for o caso.

1.3.2.2. A ACSERPROACF SSL mantém as informações acima sempre atualizadas.

1.3.3 Prestador de Serviço de Suporte

1.3.3.1 A ACSERPROACF SSL utiliza como prestador de serviço de suporte o Serviço federal de Processamento de Dados (SERPRO) em suas operações;

1.3.3.2 PSS são entidades utilizadas pela AC ou pela AR para desempenhar as atividades descritas abaixo:
a) disponibilização de infra-estrutura física e lógica;
b) disponibilização de recursos humanos especializados; ou
c) disponibilização de infra-estrutura física e lógica e de recursos humanos especializados.

1.3.3.3 A ACSERPROACF SSL mantém as informações acima atualizadas.

1.3.4. Titulares de Certificado

Os Titulares de Certificados desta PC ACSERPROACF SSL A1 são pessoas físicas ou jurídicas autorizadas pela AR vinculada a receber um certificado digital emitido pela ACSERPROACF SSL, 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 admitirem o uso de certificado digital de um determinado tipo, contemplado pela ICP-Brasil, devem aceitar qualquer certificado de mesmo tipo, ou superior, emitido por qualquer AC credenciada pela AC Raiz.

1.3.5.3 Os certificados emitidos sob esta PC pela ACSERPROACF SSL são apropriados ao uso apenas nas aplicações apresentadas na tabela descrita a seguir:

Política de Certificado	Aplicações Apropriadas
PC ACSERPROACF SSL A1	Certificados emitidos sob essa política são considerados adequados para assinatura eletrônica, irretratabilidade, integridade e autenticação. Podem ser usados nas seguintes aplicações: • Confirmação de Identidade na web; • Correio eletrônico; • Transações On-Line; • Redes privadas virtuais (VPN); • Transações eletrônicas; • Criação de chave de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.3.5.4 Certificados de tipo A1 são utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.
1.3.5.5. Não se aplica.
1.3.5.6. Não se aplica.

1.4. DADOS DE CONTATO

Esta PC é administrada pelo Centro de Certificação Digital do SERPRO, CCD-SERPRO, localizado no seguinte endereço:

SGAN 601 Módulo V
Bairro: Asa Norte
CEP: 70.836-900
Brasília / DF

Pessoas de Contato.

Nome: PEDRO MOACIR RIGO MOTTA
CENTRAL DE SERVIÇOS SERPRO (CSS)
Telefone: 0800-7282323

E-mail de Contato.
certificados@serpro.gov.br

2. DISPOSIÇÕES GERAIS

Os itens seguintes estão descritos da DPC ACSERPROACF SSL.

2.1. OBRIGAÇÕES E DIREITOS

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

Os itens seguintes estão descritos na DPC ACSERPROACF SSL.

3.1.6. Procedimento para resolver disputa de nomes

3.1.7. Reconhecimento, autenticação e papel de marcas registradas

3.1.8. Método para comprovar a posse de chave privada

3.1.9. Autenticação da identidade de um indivíduo

3.1.9.1. Documentos para efeitos de identificação de um indivíduo

3.1.9.2. Informações contidas no certificado emitido para um indivíduo

3.1.10. Autenticação da identidade de uma organização

3.1.10.1. Disposições Gerais

3.1.10.2. Documentos para efeitos de identificação de uma organização

3.1.10.3. Informações contidas no certificado emitido para uma organização

3.1.11. Autenticação da identidade de equipamento ou aplicação

3.1.11.1. Disposições Gerais

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

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

3.2. Geração de novo par de chaves antes da expiração do atual

3.3. Geração de novo par de chaves após expiração ou revogação

3.4. Solicitação de Revogação

4. REQUISITOS OPERACIONAIS

Os itens seguintes estão descritos na DPC ACSERPROACF SSL.

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

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

5.2. Controles Procedimentais

5.2.1. Perfis qualificados

5.2.2. Número de pessoas necessário por tarefa

5.2.3. Identificação e autenticação para cada perfil

5.3. Controles de Pessoal

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

5.3.2. Procedimentos de verificação de antecedentes

5.3.3. Requisitos de treinamento

5.3.4. Freqüência e requisitos para reciclagem técnica

5.3.5. Freqüência e seqüência de rodízio de cargos

5.3.6. Sanções para ações não autorizadas

5.3.7. Requisitos para contratação de pessoal

5.3.8. Documentação fornecida ao pessoal

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, são definidas as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo a PC ACSERPROACF SSL A1.

São definidos também outros controles técnicos de segurança utilizados pela DPC ACSERPROACF 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.

6.1.1.2 O Titular do Certificado gera a chave utilizando aplicativos com esta finalidade. 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 ACSERPROACF SSL recomenda que seja feito backup da chave privada, evitando assim perda do certificado.
- A ACSERPROACF SSL 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 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 é gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL[1], no meio de armazenamento definido para cada tipo de certificado A1 previsto pela ICP-Brasil.

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.

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

6.1.2. Entrega da chave privada à entidade titular

Item não aplicável.

6.1.3. Entrega da chave pública para o emissor de certificado

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

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 ACSERPROACF SSL, 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) Página *web* da ACSERPROACF SSL: https://certificados.serpro.gov.br/acserproacfssl
c) Outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

6.1.5.1.1 O tamanho das chaves criptográficas associadas aos certificados emitidos pela SERPROACF SSL são os seguintes é de, no mínimo, 2048 (dois mil e quarenta e oito) bits;

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

6.1.7 Verificação da qualidade dos parâmetros

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

6.1.8 Geração de chave por *hardware ou software*

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

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

Os certificados emitidos nesta PC tem ativado os bits digitalSignature, nonRepudiation e keyEncipherment.

6.2. Proteção da Chave Privada

Neste item são definidos os requisitos de proteção das chaves privadas de certificados emitidos segundo a PC SERPROACF.

6.2.1. Padrões para módulo criptográfico

Os Titulares de Certificado 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
Item não aplicável.

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

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

6.2.4.1 Qualquer titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.
6.2.4.2 A ACSERPROACF SSL responsável pela PC não mantém cópia de segurança de chave privada de titular.
6.2.4.3 A cópia de segurança deverá ser armazenada cifrada por algoritmo simétrico aprovado pelo documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [1] e protegida com um nível de segurança não inferior àquele definido para a chave original.
6.2.4.4 A cópia de segurança deverá ser protegida por "senha".

6.2.5 Arquivamento de chave privada

6.2.5.1 Item não aplicável, uma vez que a ICP-Brasil não admite o arquivamento de chaves privadas de assinatura digital.
6.2.5.2 Define-se arquivamento como o armazenamento da chave privada para seu uso futuro, após o período de validade do certificado correspondente.

6.2.6 Inserção de chave privada em módulo criptográfico

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

6.2.7. Método de ativação de chave privada

A chave privada é ativada, mediante 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 meses.

6.2.8. Método de desativação de chave privada

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

6.2.9 Método de destruição de chave privada

A eliminação da chave da mídia armazenadora do certificado deve ser feita através de opções disponibilizadas pelo "browser" utilizado para gerar o par de chaves. A opção permite apagar a chave privada.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

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

6.3.2 Períodos de uso para as chaves pública e privada

6.3.2.1 As chaves privadas dos respectivos Titulares são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas poderão ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2 Não se aplica.

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

6.4 Dados de Ativação

6.4.1 Geração e instalação dos dados de ativação

Item não aplicável.

6.4.2 Proteção dos dados de ativação

Item não aplicável.

6.4.3 Outros aspectos dos dados de ativação

Item não aplicável.

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

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

- Senha de *bios* ativada;
- Controle de acesso lógico ao sistema operacional;
- Existência de uso de senhas fortes;
- Diretivas de senha e de bloqueio de contas;
- Antivírus, antitrojan e antispyware instalados, atualizados e habilitados;
- Firewall pessoal ou corporativo ativado, com permissões de acesso mínimas necessárias às atividades;
- Sistema operacional mantido atualizado, com aplicação de correções necessárias (patches, hotfix, etc..)
- Proteção de tela acionada no máximo após cinco minutos de inatividade e exigindo senha do usuário para desbloqueio.

6.5.2 Classificação da segurança computacional

Item não aplicável.

6.6. Controles Técnicos do Ciclo de Vida

Item não aplicável.

6.6.1. Controles de desenvolvimento de sistema

Item não aplicável.

6.6.2 Controles de gerenciamento de segurança

Item não aplicável.

6.6.3 Classificações de segurança de ciclo de vida

Item não aplicável.

6.7. Controles de Segurança de Rede

Item não aplicável.

6.8 Controles de Engenharia do Módulo Criptográfico

Os Titulares de Certificado devem garantir que o módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1], para os certificados emitidos sob esta PC.

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 ACSERPROACF SSL, segundo esta PC, 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 SERPROACF, segundo esta PC, implementam a versão 3 de certificado definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2 Extensões de certificado

7.1.2.1. Neste item, a PC ACSERPROACF 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 SERPROACF;
b) **"*Key Usage*", crítica:** somente os bits **digitalSignature**, **nonRepudiation** e **keyEncipherment** são ativados;
c) **"*Certificate Policies*"**, **não crítica:** o campo ***policyIdentifier*** contém o OID **2.16.76.1.2.1.89,** o campo ***policyQualifiers*** contém o endereço URL *da* página *Web e* http://repositorio.serpro.gov.br/docs/dpcacserproacfssl.pdf com a DPC da ACSERPROACF SSL;
d) **"*CRL Distribution Points*", não crítica**: contém o endereço URL da página Web onde se obtém a LCR da ACSERPROACF SSL:
   - http://repositorio.serpro.gov.br/lcr/acserproacfssl.crl;e
   - http://certificados2.serpro.gov.br/lcr/acserproacfssl.crl.
e) **"*Authority Information Access*", não critica**, contendo o método de acesso ***id-ad-caIssuer***, utilizando o protocolo de acesso HTTP para a recuperação da cadeia de certificação no seguinte endereço:
   - http://ccd.serpro.gov.br/cadeias/acserproacfssl.p7b.

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

a) Para **certificados de Equipamento e Aplicação**, 4 (quatro) campos *"otherName"*, obrigatórios, contendo:
   i. **OID = 2.16.76.1.3.8 e conteúdo =** nome empresarial constante no CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, se o certificado for de pessoa jurídica.
   ii. **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;
   iii. **OID = 2.16.76.1.3.2 e conteúdo** = nome do responsável pelo certificado;
   iv. **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 subseqüentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11(onze) posições subseqüentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subseqüentes, o número do RG do responsável; nas 10 (dez) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF.

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

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

b) Quando os números de CPF, NIS (PIS, PASEP ou CI), RG, CNPJ, CEI, ou Título de Eleitor não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero";
c) Se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF. O mesmo ocorre para o campo de município e UF, se não houver número de inscrição do Título de Eleitor;
d) Quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente. No caso de múltiplas habilitações profissionais, deverão ser inseridos e preenchidos os campos (OID) correspondentes às identidades profissionais apresentadas;
e) Todas informações de tamanho variável referentes a números, tais como RG, devem ser preenchidas com caracteres "zero" a sua esquerda para que seja completado seu máximo tamanho possível;
f) As 10 (dez) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF do Título de Eleitor;
g) Apenas os caracteres de A a Z e de 0 a 9 poderão ser utilizados, não sendo permitidos caracteres especiais, símbolos, espaços ou quaisquer outros.

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

7.1.2.6. A ACSERPROACF SSL implementa as seguintes extensões, definidas como opcional pela ICP-Brasil:

a) **"*SubjectAlternativeName*", não critica**, com o seguinte OtherName:
   - O campo "*rfc822Name*" contendo o endereço de email do titular do certificado;
   - O campo "DNSName" contendo lista de URLs alternativas indicadas pelo solicitante do certificado, habilitando o certificado para uso com múltiplos domínios;

b) **"*Extended-key-usuage*", não critica** contendo os seguintes valores:
   - *"server authentication"* (OID = 1.3.6.1.5.5.7.3.1);
   - *"client authentication"* (OID = 1.3.6.1.5.5.7.3.2).

7.1.2.7. Não se aplica.

7.1.3 Identificadores de algoritmo

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

7.1.3.1.1 Os certificados emitidos pela 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

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 os certificados pessoa física:

- Para o certificado de equipamento, o identificador CN conterá o DNS oficial do equipamento:

  C = BR
  O = ICP-Brasil
  OU= Autoridade Certificadora SERPROACF SSL
  OU = *Nome da AR responsável pela aprovação do certificado*
  OU = Equipamento A1
  CN = *nome DNS oficial do equipamento (para servidores WWW)*

- Para o certificado de aplicação, o identificador CN conterá o nome da aplicação:

  C = BR
  O = ICP-Brasil
  OU= Autoridade Certificadora SERPROACF SSL
  OU = *Nome da AR responsável pela aprovação do certificado*
  OU = Aplicacao A1
  CN = *nome da aplicação*

- Para o certificado COMPE, o identificador CN do certificado de aplicação conterá as seguintes informações:

  C=BR
  O=ICP-Brasil
  OU=IF-AAAAAAAA
  OU=SSSSS-BBBBBBBBBB
  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 ECO, o identificador CN do certificado de aplicação conterá as seguintes informações:

  C=BR
  O=ICP-Brasil
  OU=*(Nome da Instituição)*
  OU=YYY Zxxx
  OU= nnnnnnn (onde nnnnnnnn é o número base do CNPJ)
  CN= O common name é composto pelo host+dominio 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 seqüência "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 cccccc é o número base do CNPJ)
  OU=CCC Pxxx ou Txxx
  OU=Nome da Instituição
  CN= O common name é composto pelo host+dominio registrado pela IF.

- 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-iiiii (Onde "iiiii" é o código do Sisbacen)
  CN= Identificação única da instituição certificada e do certificado (ex: P ou T + número seqüencial, 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 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.

7.1.5. Restrições de nome

7.1.5.1. Não se aplica.

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

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

Tabela 3 - Caracteres especiais admitidos em nomes

7.1.6 OID (*Object Identifier*) de Política de Certificado
O OID atribuído à esta Política de Certificado é: 2.16.76.1.2.1.89

7.1.7 Uso da extensão *"Policy Constraints"*
Item não aplicável.

7.1.8 Sintaxe e semântica dos qualificadores de política
Nos certificados emitidos segundo esta PC, o campo **policyQualifiers** da extensão "*Certificate Policies*" contém o endereço da página *Web* (URL) com a DPC da ACSERPROACF SSL, a saber: http://repositorio.serpro.gov.br/docs/dpcacserproacfssl.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 SERPROACF SSLsegundo 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 ACSERPROACF SSL 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 ACSERPROACF SSL; e
b) **"*CRL Number*", não crítica:** contém número seqüencial para cada LCR emitida.

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

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

8.1. PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO

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

8.2. POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO

A cada nova versão, esta PC é publicada na página *Web* da ACSERPROACF SSL *http://repositorio.serpro.gov.br/docs/acserproacfssl.pdf*.

8.3 PROCEDIMENTOS DE APROVAÇÃO

Esta PC foi submetida à aprovação da ACSERPRO, que por sua vez submeteu ao CG da ICP-Brasil, durante o processo de credenciamento da SERPROACF, conforme o estabelecido no documento "Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil". Como parte desse processo, além da conformidade com os documentos definidos pela ICP-Brasil, foi verificada a compatibilidade entre esta PC e a DPC da SERPROACF.

9. DOCUMENTOS REFERENCIADOS

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

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

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

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