www.serpro.gov.br

Política de Certificados

Serpro-SRF

Certificados tipo A3

(PCSerpro-SRFA3)

Credenciada pela ACSRF e ICP-Brasil

Soluções para um Brasil de Todos SERPRO

ÍNDICE

1. Introdução

1.1 Visão Geral

Esse documento é a Política de Certificados (PC) da Autoridade Certificadora do Serpro-SRF (ACSerpro-SRF) para certificados de assinatura digital do tipo A3, doravante denominada PCSerpro-SRFA3, implementada sob a Declaração de Práticas de Certificação da Autoridade Certificadora do Serpro-SRF (DPC da ACSerpro-SRF).

Esta PC é dirigida a gerentes, profissionais de Tecnologia da Informação (TI) da comunidade, e demais usuários, os quais têm necessidade de verificar a confiabilidade da ACSerpro-SRF e determinar a adequabilidade dos certificados Serpro-SRF do tipo A3 às suas exigências de segurança.

1.2 Identificação

Esta PC obedece as recomendações da ICP-Brasil para a emissão de certificados de assinatura digital do tipo A3.

O OID deste documento é: 2.16.76.1.2.3.4

1.3 Comunidade e Aplicabilidade

1.3.1 ACSerpro-SRF

O SERPRO, empresa subordinada ao Ministério da Fazenda, opera nas instalações do Centro de Certificação Digital do SERPRO (CCD-SERPRO) a ACSerpro-SRF como uma das Autoridades Certificadoras que compõem a Infra-estrutura de Chaves Públicas Brasileira, ICP-Brasil.

A ACSerpro-SRF se destina a emitir certificados para clientes que necessitam utilizar os certificados e-CPF, exclusivo para pessoa física, e-CNPJ, exclusivo para pessoa jurídica.

Esta PC é implementada pela ACSerpro-SRF cuja DPC (DPC da ACSerpro-SRF) encontra-se publicada na página *Web* da mesma, conforme item 2.6.1.

1.3.2 Autoridades de Registro

Os responsáveis pela função de Autoridade de Registro, são os seguintes;

- AR SERPRO
- AR SRF
- IDORT / RJ

Os endereços estão publicados na página https://ccd.serpro.gov.br/acserprosrf

É função da AR verificar, autorizar e submeter requisições de certificados e requisições de revogação de certificados, sempre em conformidade com esta Política de Certificado. Também é sua função receber, conferir e autenticar a documentação exigida conforme item 3.1.9 desta PC, além de orientar os Titulares de Certificados nos processos de solicitação de seus certificados.

O operador da AR acata as obrigações a ele impostas por esta Política de Certificados e pela Declaração de Práticas de Certificação da ACSerpro-SRF, DPC da ACSerpro-SRF, as quais descrevem em linhas gerais todos os seus procedimentos.

A PC será atualizada sempre que houver o credenciamento de mais uma AR vinculada à ACSERPRO.

1.3.3 Titulares de Certificado

Os Titulares de Certificados desta PCSerpro-SRFA3 são pessoas físicas ou jurídicas autorizadas pela AR a receber um certificado digital emitido pela ACSerpro-SRF, para sua própria utilização.

Em sendo o titular do certificado pessoa jurídica, será designado pessoa física como responsável pelo certificado, que será a detentora da chave privada.

Preferencialmente será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um de seus representantes legais.

Em se tratando de certificado emitido para equipamento ou aplicação, o titular será a pessoa física ou jurídica solicitante do certificado, que deverá indicar o responsável pela chave privada.

1.3.4 Aplicabilidade

Os certificados emitidos sob esta PC pela ACSerpro-SRF estão definidos na tabela a seguir:

Nome do Certificado	Tipo	Apropriado para
e-CPF	A3	Pessoas Físicas
e-CNPJ	A3	Pessoas Jurídicas

Esses certificados se destinam à utilização em assinatura digital, não repúdios, garantia de integridade da informação, autenticação de seu titular.

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 com requisitos de segurança mais rigorosos, emitido por qualquer Autoridade Certificadora credenciada pela AC-Raiz.

1.3.4.1 Aplicações Apropriadas

Os certificados emitidos sob esta PC pela ACSerpro-SRF são apropriados ao uso apenas nas aplicações apresentadas na tabela descrita a seguir (tabela 2).

Tabela 2 – Aplicações Apropriadas

Política de Certificado	Aplicações apropriadas
PCSerproSRFA3	Certificados emitidos sob essa política são considerados adequados para assinatura eletrônica, irretratabilidade, integridade e autenticação pessoal. Eles podem ser usados nas aplicações abaixo:

	• Confirmação de Identidade na Web; • Correio Eletrônico; • Transações on-line; • Redes privadas virtuais (VPN); • Transações eletronicas; • Cifração de chaves de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.3.4.2 Aplicações Proibidas

O uso de certificados e chaves privadas emitidas sob esta PC está limitado às aplicações especificadas no item 1.3.4.1. Todas as demais aplicações são proibidas.

1.4 Dados de Contato

1.4.1 Organização da Administração da PCSerproSRFA3

Esta PC é administrada pelo Centro de Certificação Digital do SERPRO, CCD-SERPRO localizado no seguinte endereço:
Rua Pacheco Leão Número 1235 – Fundos
Bairro. Jardim Botânico
CEP. 22.460.030
Rio de Janeiro – RJ.

1.4.2 Pessoas de Contato

Nome: Márcia Paulina Souza
Telefone: (21) 2529-3611 ou 2529-3612
E-mail: marcia-paulina.souza@serpro.gov.br
Fax: (21) 529-3360

2. Definições Gerais

Este capítulo possui definições acerca das obrigações da ACSerpro-SRF, de suas Autoridades de Registro (AR), de seus Titulares de Certificado e Usuários, e demais assuntos relacionados com a legislação e solução de conflitos.

2.1 Obrigações e Direitos

2.1.1 Obrigações da Autoridade Certificadora

A ACSerpro-SRF deve:

1) Operar de acordo com:
   - esta PC;
   - DPC da ACSerpro-SRF;
   - Política de Segurança da ACSerpro-SRF;
   - Política de Segurança da ICP-Brasil.
2) Gerar e gerenciar o seu par de chaves criptográficas;
3) Assegurar a proteção de suas chaves privadas;
4) Notificar a AC Raiz e a AC-SRF, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do seu certificado;
5) Notificar os seus usuários quando ocorrer suspeita de comprometimento de sua chave, emissão de novo par de chaves e correspondente certificado, ou o encerramento de suas atividades;
6) Distribuir o seu próprio certificado;
7) Emitir, expedir e distribuir os certificados de AR vinculadas e os certificados dos usuários finais;
8) Informar a emissão do certificado ao respectivo solicitante;
9) Revogar, quando necessário, os certificados por ela emitidos;
10) Emitir, gerenciar e publicar suas Listas de Certificados Revogados (LCR);
11) Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
12) Publicar em sua página Web a DPC da ACSerpro-SRF e suas PC aprovadas;
13) Adotar as medidas de segurança e controle previstas na DPC, PC e Política de Segurança da ACSerpro-SRF, envolvendo seus processos, procedimentos e atividades, observada as normas, critérios, práticas e procedimentos da ICP-Brasil;
14) Manter a conformidade dos processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
15) Manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
16) Manter e testar regularmente seu Plano de Continuidade do Negócio;
17) Informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pela ACSerpro-SRF;
18) Armazenar, pelo prazo estipulado pela ICP-Brasil, cópia dos certificados dos Titulares;
19) Tomar as medidas cabíveis para assegurar que usuários e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações;

20) Não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;
21) Atender à Instrução Normativa número 222 de 11.10.2002 no seu Art. 10:
22) Manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, e exigir sua manutenção pelas AC de nível subseqüente ao seu, quando estas estiverem obrigadas a contratá-lo, de acordo com as normas do Comitê Gestor da ICP-Brasil.

2.1.2 Obrigações das AR

Pela adesão às práticas descritas nesta PC, os responsáveis pela AR ficam cientes das obrigações a que estão submetidos.

São obrigações dos responsáveis das AR:

1) Operar de acordo com:
   - Esta PC;
   - A DPC da ACSerpro-SRF;
   - A Política de Segurança da ACSerpro-SRF;
   - A Política de Segurança da ICP-Brasil.

2) Receber solicitações de emissão ou de revogação de certificados;
3) Receber e guardar as cópias dos documentos de identificação solicitados dos Titulares de Certificados conforme indicado no item 3.1.9 desta PC;
4) Confirmar a identidade dos solicitantes de certificado de seu domínio conforme indicado no item 3.1.9 desta PC;
5) Receber o Termo de Titularidade e Responsabilidade ou Termo de Titularidade assinado pelo Titular do Certificado;
6) Conferir a exatidão das informações contidas no Termo de Titularidade e Responsabilidade ou de Titularidade;
7) Assinar o Termo de Titularidade e Responsabilidade ou de Titularidade do Titular do Certificado, confirmando sua autenticidade;

8) Encaminhar a solicitação de emissão ou de revogação de certificado à ACSerpro-SRF utilizando VPN (virtual private network – rede privativa virtual), SSL (secure socket layer – protocolo de comunicação seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade;

9) Utilizar VPN (virtual private network – rede privativa virtual), SSL (secure socket layer – protocolo de comunicação seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade, ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;
10) Informar aos Titulares de Certificados a emissão ou a revogação de seus certificados;
11) Disponibilizar os certificados emitidos pela ACSerpro-SRF aos seus respectivos solicitantes;

12) Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
13) Manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC-SRF;
14) Manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil;
15) Oferecer treinamento aos seus agentes de registro, especialmente quanto ao reconhecimento de assinaturas e validade dos documentos apresentados na forma dos itens 3.1.8 e 3.1.9.

2.1.3 Obrigações de Titulares de Certificado

Aceitando as práticas descritas nesta Política de Certificados (PCSerpro-SRFA3), os Titulares de Certificado ficam cientes das obrigações a eles impostas pela mesma. Os Titulares de Certificado, incluindo os responsáveis pela AR e pela ACSerpro-SRF, são responsáveis por:

1) Fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
2) Garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
3) Utilizar os seus certificados e chaves privadas em aplicações aprovadas e de modo apropriado, conforme o previsto nesta PC;
4) Conhecer os seus direitos e obrigações, contemplados por esta PC, pela DPC da ACSerpro-SRF e por outros documentos aplicáveis da ICP-Brasil;
5) Notificar imediatamente a AR de qualquer erro ou defeito nos certificados , ou de qualquer mudança subseqüente na informação do certificado;
6) Informar à ACSerpro-SRF, através de sua AR, qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente;
7) Estar ciente das obrigações e responsabilidades estipuladas nesta Política de Certificados sob a qual seu certificado é emitido, assinando o Termo de Titularidade ou Termo de Titularidade e Responsabilidade.

Nota: Em se tratando de certificado emitido para pessoa jurídica, esta obrigações se aplicam ao responsável pelo uso do certificado.

2.1.4 Direitos do Usuário de Certificado (Terceira Parte Confiável)

Considera-se Usuário de Certificado a entidade que confia no teor, validade e aplicabilidade do certificado digital.

Constituem direitos do Usuário de Certificado:

1) Recusar a utilização do certificado para fins diversos dos previstos nesta PC;
2) Verificar, a qualquer tempo, a validade do certificado. Um certificado emitido pela ACSerpro-SRF é considerado válido quando:
   - Não constar da LCR da ACSerpro-SRF;
   - Não estiver expirado; e
   - Puder ser verificado com o uso de certificado válido da ACSerpro-SRF;

O não exercício desses direitos não afasta a responsabilidade da ACSerpro-SRF e do titular do certificado.

2.1.5 Obrigações do Repositório

O repositório da ACSerpro-SRF está disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

O repositório está instalado em sala com controle de acesso biométrico, há controle de acesso lógico dual, o sistema possui sistema de configuração para eliminação de vulnerabilidades, conforme orientações dos fabricantes e de instituições de segurança reconhecidas. Existe sistema de identificação de intrusão na rede em que o equipamento está conectado, como também há proteção por firewall. O sistema interno de arquivos e diretório do repositório possui controle de permissão de acesso.

2.2 Responsabilidades

2.2.1 Responsabilidades da ACSerpro-SRF

A ACSerpro-SRF responde pelos danos a que der causa.

2.2.2 Responsabilidades das AR

A AR será responsável pelos dados a que der causa.

2.3 Responsabilidade Financeira

2.3.1 Indenização devida pelos Usuários de Certificados

Não existe situação específica de utilização do certificado da ACSerpro-SRF que requeira prática de indenização pelos Usuários de Certificados, exceto na prática de ato ilícito.

2.3.2 Relações Fiduciárias

A ACSerpro-SRF ou AR vinculada indenizará integralmente os danos o que der causa. Em situações justificáveis, pode ocorrer limitação da indenização, quando o titular do certificado for pessoa jurídica.

2.3.3 Processos Administrativos

Os processos administrativos cabíveis, relativos às operações da ACSERPRO-SRF e das AR vinculadas estão sujeitas à legislação aplicável que suporta esta Política de Certificados, além da legislação interna do SERPRO que mantém o CCD SERPRO.

2.4 Interpretação e Execução

2.4.1 Legislação

Segue abaixo relação de documentos que suportam esta Política de Certificados:

1) Resoluções do Comitê Gestor da ICP-Brasil.
2) Decreto nº 3.996, de 31 de outubro de 2001. Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.
3) Medida Provisória nº 2.200-2, de 24 de Agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências.
4) Decreto nº 3.872, de 18 de Julho de 2001. Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva, sua Comissão Técnica Executiva e dá outras providências.
5) Decreto nº 3.587, de 05 de setembro de 2000. Estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal - ICP-Gov, e dá outras providências.
6) Decreto nº 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
7) Lei 9.983 de 14 de julho de 2000 Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências.
8) Instrução Normativa Número 222 de 11.10.2002 da Secretaria da Receita Federal.

2.4.2 Forma de interpretação e notificação

No caso de uma ou mais das disposições desta PC ser, por qualquer razão, considerada inválida, ilegal, ou não aplicável, somente essa disposição será afetada, todas as demais permanecem válidas dentro do escopo de abrangência deste documento. A ACSerpro-SRF promoverá a correção do item em desacordo, no prazo de 05 dias.

As práticas descritas nesta PC não prevalecerão sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

Todas as solicitações, notificações ou quaisquer outras comunicações necessárias sujeitas às práticas descritas na PC deverão ser realizadas por iniciativa da ACSerpro-SRF através de seus responsáveis.

2.4.3 Procedimentos de resolução de disputas

No caso de um conflito entre esta PC e outras políticas, planos, acordos, contratos ou procedimentos onde o assunto da disputa está entre esta PC e:

1) Um acordo operacional, esta PC prevalecerá;
2) Um Termo de Titularidade e Responsabilidade ou de Titularidade, esta PC prevalecerá;
3) Qualquer política, plano, procedimentos ou qualquer outra documentação operacional ou documentação de práticas, esta PC prevalecerá.

No caso de um conflito entre esta PC e as resoluções do Comitê Gestor da ICP-Brasil, prevalecerão sempre as normas, critérios, práticas e procedimentos estabelecidos pelo CG da ICP-Brasil.

2.5 Tarifas de Serviço

As tarifas previstas a serem cobradas dos Titulares de Certificados serão descritas a seguir.

2.5.1 Tarifas de emissão ou renovação de certificados

Os valores praticados, constam em contrato entre o Serpro e os solicitantes do certificado.

2.5.2 Tarifas de acesso aos certificados

Não há tarifa que incida sobre este serviço.

2.5.3 Tarifas de revogação ou acesso à informação de estado

Não há tarifa que incida sobre este serviço.

2.5.4 Tarifas para outros serviços como informação de política

Não há tarifa que incida sobre este serviço.

2.5.5 Política de reembolso

A Política de reembolso está descrita em contrato entre o Serpro e os solicitantes do certificado.

2.6 Publicação e Repositórios

2.6.1 Publicação de informações da ACSerpro-SRF

A ACSerpro-SRF mantém página *Web* https://ccd.serpro.gov.br/acserprosrf que contém as seguintes informações:

1) PC ACSerpro-SRF A3:
   - https://ccd.serpro.gov.br/acserprosrf/docs/pcserprosrfA3.pdf;
2) DPC da ACSerpro-SRF:
   - https://ccd.serpro.gov.br/acserprosrf/docs/dpcacserprosrf.pdf
3) LCR:
   - http://ccd.serpro.gov.br/lcr/acserprosrf.crl
4) Certificado da ACSerpro-SRF
5) Certificado da AC-SRF;
6) Certificado da AC Raiz da ICP-Brasil;
7) Certificados emitidos pela ACSerpro-SRF;
8) Os endereços das instalações técnicas das AR vinculadas.

A disponibilidade da página *Web* é de, no mínimo, de 99% (noventa e nove por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.6.2 Freqüência da publicação

Os certificados emitidos pela ACSerpro-SRF são publicados imediatamente após a sua emissão. Quando revogados, os certificados são publicados em LCR. A freqüência de publicação da LCR sob esta política é a cada 24 (vinte e quatro) horas. A LCR utiliza como repositório uma página *Web* http://ccd.serpro.gov.br/lcr/acserprosrf.crl conforme descrito no item 2.6.4.

Novas versões da Política de Certificados (PC) e da correspondente DPC são carregadas prontamente na página *Web* da ACSerpro-SRF,

https://ccd.serpro.gov.br/acserprosrf/docs/pcserprosrfA3.pdf e https://ccd.serpro.gov.br/acserprosrf/docs/dpcacserprosrf.pdf, através de procedimentos seguros.

2.6.3 Controle de acesso

Não há nenhum controle de acesso na leitura desta PC ou da DPC da ACSerpro-SRF.

São utilizados recursos apropriados para restringir a possibilidade de escrita ou modificação destes documentos a pessoal autorizado.

A equipe da ACSerpro-SRF possui os privilégios necessários para reposição de PC e desta DPC por novas versões, e para gerar e publicar LCR, consistentes com suas respectivas funções.

2.6.4 Repositórios

O repositório das informações publicadas pela ACSerpro-SRF pode ser acessado através da página https://ccd.serpro.gov.br/acserprosrf , que atende aos seguintes requisitos:

1) Disponibilidade – aquela definida no item 2.6.1;
2) Protocolos de acesso – HTTP e HTTPS;
3) Requisitos de segurança – obedece aos requisitos definidos no item 5.

2.7 Auditoria de Conformidade

A AC Raiz da ICP-Brasil realiza auditoria de conformidade nas instalações da ACSerpro-SRF previamente ao seu credenciamento pela AC-Raiz e à sua habilitação pela AC-SRF. Adicionalmente, a ACSerpro-SRF de nível imediatamente subseqüente ao da AC-SRF, para fins de continuidade do credenciamento, apresenta anualmente relatório de auditoria fornecido por empresa de auditoria especializada e independente, contratada pela ACSerpro-SRF e autorizada pela AC Raiz. A ACSerpro-SRF realiza auditorias de conformidade anuais nas AR operacionais e disponibiliza à AC-SRF os relatórios destas auditorias.

Auditorias intempestivas podem ser executadas por qualquer das entidades acima descritas a qualquer uma das entidades à ela subordinadas.

Os itens seguintes desta PC detalham os aspectos relacionados a esse processo de auditoria.

2.7.1 Freqüência de auditoria de conformidade de entidade

A ACSerpro-SRF conduz anualmente auditorias de conformidade em todas as entidades à ela vinculadas, podendo também executar, a qualquer momento, auditorias intempestivas.

2.7.2 Identidade/Qualificações do Auditor

Os relatórios de auditoria das AR executados pela ACSerpro-SRF são feitos por equipe com comprovada experiência em serviços de auditoria e tecnologias de certificação. Estas auditorias podem também ser executadas por empresa de auditoria especializada e independente autorizada pela AC-Raiz.

2.7.3 Relação entre Auditor e Parte Auditada

No caso de contratação de auditoria independente, o auditor e a parte auditada não devem possuir qualquer relação atual ou planos de relação financeira, legal, ou outra que poderia resultar em um conflito de interesse, além da função de auditoria.

2.7.4 Tópicos cobertos pela Auditoria

Os tópicos cobertos pela auditoria executada pela ACSerpro-SRF em suas entidades vinculadas incluirão, mas não se limitarão a conformidade com:

1) Política de segurança;
2) Segurança física;
3) Avaliação de tecnologia;
4) Administração dos Serviços da ACSerpro-SRF;
5) Investigação de pessoal;
6) PC e DPC implementadas;
7) Contratos;
8) Considerações de privacidade.

2.7.5 Medidas adotadas em caso de não conformidade

Os relatórios de auditoria são submetidos à ACSerpro-SRF e disponibilizados para a AC-SRF. Quando encontradas irregularidades, a ACSerpro-SRF prontamente implementa as correções apropriadas acompanhando suas implementações.

2.7.6 Comunicação de Resultados

A ACSerpro-SRF entregará os relatórios completos das auditorias à AC-SRF, que por sua vez os entregará à AC-Raiz.

É considerado que os relatórios completos de auditoria são informações sigilosas, devendo ser protegidos conforme as exigências de confidencialidade desta PC e dos documentos contratuais aplicáveis.

2.8 Sigilo

Os Titulares de Certificados emitidos para pessoas físicas ou os responsáveis pelo uso de certificados para pessoas jurídicas serão responsáveis pela geração, manutenção e sigilo de suas respectivas chaves privadas, bem como pela divulgação ou utilização indevida dessas mesmas chaves. Os certificados do tipo A3, objetos desta PC, possuem chaves geradas em cartões inteligentes (*Smart Cards*) ou token com capacidade de geração de chaves criptográficas. A segurança da chave privada repousa, nesse caso, na proteção da senha de acesso ao cartão ou token.

O Titular do Certificado deve observar procedimentos básicos de segurança, tais como:

1) Nunca fornecer a senha a terceiros;
2) Utilizar senhas de, no mínimo, 8 caracteres;
3) Montar senhas com caracteres numéricos e alfanuméricos;
4) Memorizar a senha e não escrevê-la.

O certificado emitido sob esta PC não é um certificado de sigilo.

2.8.1 Tipos de Informações Sigilosas

Todas as informações coletadas, geradas, transmitidas e mantidas pela ACSerpro-SRF são consideradas sigilosas, exceto os certificados de chaves públicas e LCR, os quais são considerados informação não sigilosa, assim como a versão desta PC e da DPC da ACSerpro-SRF.

Como princípio geral, nenhum documento, informação ou registro fornecido à ACSerpro-SRF ou às AR deverá ser divulgado.

2.8.2 Tipos de Informações não sigilosas

As informações não sigilosas que podem ser divulgadas pela ACSerpro-SRF incluem:

1) Os certificados e as LCR emitidos;
2) Informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;
3) Esta PC;
4) A DPC da ACSerpro-SRF;
5) Versões públicas de Políticas de Segurança;
6) Resultados finais de auditorias.

2.8.3 Divulgação de Informação de Revogação/Suspensão de Certificados

Informações de estado de certificados são fornecidos através de consulta à LCR aplicável.

As razões para revogação de um certificado sempre serão informadas para o seu titular, e serão tornadas públicas desde que haja autorização expressa deste.

A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

2.8.4 Quebra de sigilo por motivos legais

Como princípio geral, nenhum documento, informação ou registro que pertençam ou estejam sob a guarda da ACSerpro-SRF e suas AR é divulgado a entidades legais ou seus funcionários, exceto quando:

1) Exista uma ordem judicial corretamente constituída; e
2) Esteja corretamente identificado o representante da lei.

2.8.5 Informações a terceiros

Nenhum documento, informação ou registro sob a guarda da ACSerpro-SRF e suas AR será fornecido a qualquer pessoa, exceto quando a pessoa que o requerer, por meio de instrumento devidamente constituído, estiver autorizada para fazê-lo e corretamente identificada.

2.8.6 Divulgação por solicitação do titular

O Titular do Certificado, ou seu representante legal, poderá ter acesso a quaisquer dos seus dados ou identificações, ou poderá autorizar a divulgação de seus registros a outras pessoas. Para tanto, a solicitação de liberação de informação deverá ser acompanhada de autorização formal do Titular do Certificado.

2.8.7 Outras circunstâncias de divulgação de informação

Não estão previstas outras circunstâncias em que poderão ser divulgadas informações sigilosas.

2.9 Direitos de Propriedade Intelectual

Todos os direitos de propriedade intelectual inclusive todos os direitos autorais em todos os certificados e todos os documentos gerados para a ACSerpro-SRF (eletrônico ou não) pertencem e continuarão sendo propriedade do SERPRO.

O Titular de Certificado concede à ACSerpro-SRF, o direito de publicar e divulgar em página *web* a chave pública que corresponde à chave privada que está sob posse do Titular de Certificado. Esta publicação ocorrerá pela incorporação da chave pública em certificado emitido pela ACSerpro-SRF. Nada nesta cláusula concede ao Titular de Certificado qualquer direito em relação ao formato ou estrutura do certificado que acompanha sua chave pública.

Direitos sobre Identificadores de Objeto (OID) atribuídos à ACSerpro-SRF após o processo de credenciamento, cabem única e exclusivamente ao ITI, designado como a AC Raiz da ICP-Brasil.

3. Identificação e Autenticação

Esta seção descreve as práticas adotadas pelas AR credenciadas pela ACSerpro-SRF na identificação e autenticação de seus Titulares de Certificado.

3.1 Registro Inicial

A AR realizará a autenticação da identidade de uma organização (item 3.1.8) e a autenticação da identidade de um indivíduo (item 3.1.9) por meio de, no mínimo, dois agentes de registro responsáveis pelo recolhimento e verificação da validade dos documentos apresentados.

3.1.1 Tipos de Nomes

No domínio da ACSerpro-SRF, o atributo sujeito nos certificados emitidos para Titulares de Certificado , são do tipo *Distinguished Name*, contendo sempre o nome no formato previsto pelo padrão ITU X.500.

Os certificados emitidos para pessoa jurídica incluem o nome da pessoa física responsável pelo seu uso. Para todos os efeitos legais, os certificados e as respectivas chaves de assinatura são de titularidade do responsável constante do certificado.

3.1.2 Necessidade de Nomes Significativos

e-CPF

O campo *Common Name* é composto do nome do Titular do Certificado, conforme consta no Cadastro de Pessoa Física.

O campo *Organizational Unit* é composto pelo texto “SRF e-CPF” para identificar os certificados do tipo e-CPF.

e-CNPJ

O campo *Common Name* é composto com o nome empresarial da pessoa jurídica, conforme consta no Cadastro Nacional da Pessoa Jurídica.

O campo *Organizational Unit* é composto pelo texto “SRF e-CNPJ” para identificar os certificados do tipo e-CNPJ.

O campo *StateOrProvince* é composto pela sigla da Unidade da Federação onde se localiza a pessoa jurídica.

O campo *Locality* é composto pelo nome da cidade onde se localiza a pessoa jurídica.

3.1.3 Regras para interpretação de vários tipos de nomes

Não existem regras específicas para interpretação de nomes no âmbito da ACSerpro-SRF.

3.1.4 Unicidade de Nomes

Esta PC estabelece que identificadores do tipo "*Distinguished Name" (DN)* serão únicos para cada titular de certificado, no âmbito da ACSerpro-SRF. Para assegurar a unicidade do campo, nos certificados e-cpf e e-cnpj é incluído o número do CPF e o número do CNPJ após o nome do titular do certificado respectivamente.

3.1.5 Procedimento para resolver disputa de nomes

No âmbito da ACSerpro-SRF não há disputa decorrente da igualdade de nomes entre solicitantes de certificados pois o nome do Titular do Certificado será formado a partir do nome constante dos cadastros da SRF, CPF ou CNPJ para certificados pessoa física ou jurídica respectivamente, acrescido do número de inscrição nestes cadastros. Este procedimento garante a unicidade de todos os nomes no âmbito da ACSerpro-SRF.

3.1.6 Reconhecimento, autenticação e papel de marcas registradas

De acordo com a legislação em vigor.

3.1.7 Método para comprovar a posse da Chave Privada

O sistema de certificação, implementado no CCD-SERPRO e utilizado pela ACSerpro-SRF no gerenciamento do ciclo de vida de seus certificados, controla e garante, de forma automática, a entrega do certificado somente ao detentor da chave privada correspondente à chave pública constante do certificado.

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. Ao recebê-la o software de certificação (SGC) procede a verificação automática da assinatura digital com uso da chave pública incluída nessa solicitação. Esse teste confirma a posse da chave privada pelo requisitante. A solicitação é então armazenada no banco de dados do SGC e possui, associado, um número de identificação. Este número é impresso no Termo de Titularidade e Responsabilidade ou de Titularidade junto com os dados da entidade solicitante. Os dados são autenticados pela AR através de documentos oficiais, efetivando a vinculação da solicitação e chave privada à entidade autenticada pela AR.

3.1.8 Autenticação da Identidade de uma Organização

O processo de autenticação da pessoa jurídica previsto nesta PC é feito por Autoridade de Registro (AR) da ACSerpro-SRF, e exige a presença física do Titular do Certificado com cópias dos documentos autenticados em cartório.

Serão exigidos os seguintes documentos comprovando a identidade da Pessoa Jurídica:

1) Prova de inscrição no Cadastro Nacional de Pessoa Jurídica (cartão CNPJ).
2) Registro comercial, no caso de empresa individual;
3) Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais ou civis, e , no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores.

No momento da solicitação do certificado de pessoa jurídica será realizada consulta prévia à situação cadastral do CNPJ da organização, junto ao cadastro da SRF. Se o CNPJ informado existir na base de dados, será verificada sua situação cadastral. Se estiver em situação que impeça o fornecimento do certificado, isto é, se estiver em situação cadastral de **INAPTO, CANCELADO ou SUSPENSO**, a solicitação do certificado não será enviada à ACSerpro-SRF.

A pessoa física responsável referida no item 3.1.1 também é identificada, na forma descrita no item seguinte.

3.1.9 Autenticação da Identidade do Indivíduo

O processo de autenticação da identidade dos Titulares de Certificado prevista nesta PC é feito por Autoridade de Registro (AR), que faz a checagem mediante a presença física do interessado e dos documentos de identificação legalmente aceitos

No momento da solicitação do certificado e-CPF será realizada consulta prévia à situação cadastral do CPF do Titular do Certificado junto ao cadastro da SRF. Se o CPF informado existir na base de dados, será verificada sua situação cadastral. Se estiver em situação cadastral **CANCELADO**, a solicitação do certificado não será enviada à ACSerpro-SRF.

Quando o titular do certificado for pessoa jurídica, deverá ser feita a confirmação de sua identidade, na forma do item 3.1.8; e de seu representante legal, mediante a apresentação dos documentos descritos no item 3.1.9.1. Neste caso, o representante legal da pessoa jurídica, juntamente com a pessoa física indicada como responsável pelo certificado, assinarão “Termo de Titularidade e Responsabilidade”.

Tanto a pessoa jurídica titular do certificado, como a pessoa física designada como responsável pelo certificado, serão responsáveis, pela correta utilização deste conforme as normas da ICP-Brasil. Será feita ainda a confirmação da identidade da pessoa física responsável pelo uso do certificado.

É mantido arquivo com o tipo e os detalhes do procedimento de identificação utilizado em cada caso.

3.1.9.1 Documentos para identificação

Deve ser apresentada uma foto recente e, os seguintes documentos acompanhados de cópia:

1. Cédula de Identidade ou Passaporte, se estrangeiro;
2. Cadastro de Pessoa Física (CPF);
3. Comprovante de residência;
4. Número de identificação Social-NIS (Cadastro do Programa de Integração Social-PIS, Cadastro do Programa de Formação do Patrimônio do Servidor Público-PASEP ou Cadastro de Contribuinte Individuais do INSS-CI), se aplicável;
5. Cadastro Especifico do INSS (CEI), se aplicável;
6. Titulo de Eleitor, se aplicável.

Os documentos acima relacionados do responsável, caso o solicitante seja incapaz.

NOTA: Entende-se por cédula de identidade as carteiras instituídas por lei, desde que contenham foto e às mesmas seja atribuída fé pública em todo o território nacional, tais como: Carteira de Identidade emitida pela Secretaria de Segurança Pública, Carteira Nacional de Habilitação, Carteira de Identidade Funcional, Carteira de Identidade Profissional.

3.1.9.2 Certificado Emitido para Pessoa Física.

Deverá ser feita a confirmação de sua identidade, na forma do item 3.1.9.1, e esta assinará Termo de Titularidade.

3.1.9.3 Certificado Emitido para Pessoa Jurídica.

Deverá ser feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos;

- Apresentação do rol de documentos elencados no item 3.1.8;
- Apresentação do rol de documentos elencados no item 3.1.9.1 do representante legal da pessoa jurídica e do responsável pelo uso do certificado; e
- Presença física do responsável pelo uso do certificado e do representante legal da pessoa jurídica e assinatura conjunta do Termo de Titularidade e Responsabilidade;

3.1.9.4 Certificado emitido para equipamentos ou aplicação.

Não se aplica aos certificados emitidos sob esta política.

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

Os Titulares de Certificado serão comunicados por Email da necessidade da renovação com uma antecedência mínima de um mês pela ACSerpro-SRF. As solicitações de renovação de certificados serão feitas pelos próprios Titulares de Certificado quando do recebimento dessa notificação, por meio eletrônico e assinada digitalmente com o uso de certificado vigente de mesmo nível de segurança, podendo repetir esse procedimento por 3 (três) ocorrências sucessivas.

3.3 Geração de novo par de chaves após revogação

Os procedimentos utilizados para confirmação da identidade de uma entidade solicitante de novo certificado, após a revogação do certificado dessa entidade, são os mesmos executados quando da solicitação do certificado.

3.4 Solicitação de revogação

Solicitações de revogação de certificados devem ser feitas em formulário específico, disponibilizado na página *Web* da ACSerpro-SRF, que deve ser preenchido e assinado pelo Titular do Certificado ou pela AR. Estas solicitações ficam arquivadas pelas AR.

A confirmação da identidade do Titular do Certificado pela AR deve ser feita com base em um dos documentos de identidade descritos no item 3.1.9 desta PC.

4. Requisitos Operacionais

Esta seção descreve as práticas operacionais seguidas pelos Titulares de Certificado, pela AR e pela ACSerpro-SRF nos processos de solicitação, emissão, aceitação e revogação de certificados, registros de auditoria e arquivamento.

4.1 Solicitação de Certificados

Os seguintes passos devem ser seguidos pelos Titulares de Certificado para a solicitação de certificados:

1) O solicitante de certificado acessa a página *Web* https://ccd.serpro.gov.br/acserprosrf da ACSerpro-SRF, seleciona uma das opções constantes em "Certificados A3" ("e-cpf" ou "e-cnpj"), lê as instruções constantes nesta página, seleciona "Avançar" na parte inferior direita da página e então seleciona a opção "Solicitar Certificado". Preenche então os dados solicitados, imprime em duas vias o Termo de Titularidade, para e-cpf, ou o Termo de Titularidade e Responsabilidade, para o e-cnpj, e envia a sua solicitação;
2) No formulário da solicitação que será preenchido será solicitada a criação de um código de acesso que será utilizado posteriormente para a busca e instalação do certificado;
3) O solicitante preenche no Termo Titularidade ou no Termo de Titularidade e Responsabilidade o número de sua solicitação recebido após o envio da mesma, e se dirige a uma das AR indicadas pela ACSerpro-SRF munido dos documentos exigidos para comprovação dos atributos de identificação constantes do certificado.

Os seguintes passos são executados pelo Agente de Registro responsável pela solicitação;

1) A validação das informações contidas no Termo de Titularidade, e se o caso, Termo de Titularidade e Responsabilidade do solicitante;
2) Assinatura por parte do solicitante e dos agentes de registro dos Termos;
3) Autenticação do agente de registro responsável pelas solicitações de emissão e de revogação de certificados mediante o uso de certificado digital com requisitos de segurança, equivalentes a de um certificado de nível A3;
4) Comprovação dos atributos de identificação constantes do certificado, conforme item 3.1;
5) Aprovação do Certificado Digital pelo agente de registro;
6) Entrega de uma via do Termo de Titularidade, e se o caso, Termo de Titularidade e Responsabilidade para o solicitante do certificado.

4.2 Emissão de Certificados

Os certificados são emitidos pela ACSerpro-SRF de acordo com os seguintes passos:

1) O responsável pela AR verifica o completo e correto preenchimento da solicitação do certificado;
2) O responsável pela AR aprova a solicitação, disponibilizando o certificado para a instalação por seu solicitante.
3) O software de AC emite automaticamente uma notificação ao solicitante informando que o certificado está disponível para busca.

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

4.3 Aceitação de Certificados

Os certificados são instalados de acordo com os seguintes passos:

1) O solicitante do certificado acessa a página https://ccd.serpro.gov.br/acserprosrf da ACSerpro-SRF, seleciona uma das opções constantes em "Certificados A3" ("e-cpf" ou "e-cnpj"), lê as instruções constantes nesta página, seleciona "Avançar" na parte inferior direita da página;
2) O solicitante seleciona a opção "Buscar Certificado" e informa o número da sua solicitação e o código de acesso definido no processo de solicitação do certificado;
3) O solicitante instala o certificado em seu cartão inteligente ou token, conferindo seus dados impressos no certificado;
4) O Titular do Certificado troca a senha de seu cartão inteligente ou token, seguindo as instruções do item 2.8 desta PC.

O recebimento de um certificado pelo Titular de Certificado e o uso subseqüente das chaves e certificado, constitui aceitação deste certificado.

No caso de certificados de pessoas jurídicas, a aceitação é feita pela pessoa física responsável pelo certificado.

Aceitando um certificado, o Titular do Certificado:

1) Concorda estar de acordo com as responsabilidades, obrigações e deveres impostos a ele pelo Termo de Titularidade ou pelo Termo de Titularidade e Responsabilidade, por esta PC e pela DPC da ACSerpro-SRF;
2) Garante que por seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada com o certificado;

Afirma que as informações do certificado fornecidas durante o processo de solicitação são verdadeiras e foram publicadas dentro do certificado com precisão.

4.4 Suspensão e Revogação de Certificados

4.4.1 Circunstâncias para revogação

A ACSerpro-SRF pode revogar um certificado por ela emitido pelos seguintes motivos:

1) Solicitação de revogação corretamente formulada do Titular do Certificado;
2) Uma solicitação de revogação validada é recebida de um terceiro autorizado, por exemplo:
   - uma determinação judicial;
3) Uma solicitação de revogação é feita por uma pessoa com procuração do Titular do Certificado.

A ACSerpro-SRF revogará obrigatoriamente um certificado por ela emitido pelos seguintes motivos:

1) Emissão imprópria ou defeituosa do certificado;
2) Uma informação contida no certificado foi alterada ou não é mais válida;
3) Comprometimento ou suspeita de comprometimento de chaves privadas ou senhas;
4) Comprometimento ou suspeita de comprometimento da mídia armazenadora de chaves privadas;
5) Encerramento das operações da ACSerpro-SRF;
6) Certificado da ACSerpro-SRF , da AC-SRF ou da AC Raiz da ICP-Brasil é revogado.

Em relação à revogação, também será observado:

1) A ACSerpro-SRF revogará, no prazo definido no item 4.4.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas pela ICP-Brasil e contidas nesta PC;

4.4.2 Quem Pode Solicitar a Revogação

Revogações podem ser feitas:

1) por solicitação do titular do certificado;
2) por solicitação do responsável pelo certificado, no caso de pessoas jurídicas;
3) por solicitação de empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;
4) pela ACSerpro-SRF;
5) por uma AR vinculada; ou
6) por determinação do CG da ICP Brasil ou da AC Raiz.

4.4.3 Procedimentos para a Revogação

O procedimento para a solicitação de uma revogação varia dependendo de quem a origina.

Quando a solicitação se origina de um Titular ela será submetida pessoalmente à AR através de documento específico existente na página da ACSerpro-SRF.

A ACSerpro-SRF estabelece que:

1) O solicitante da revogação sendo o Titular do Certificado de um certificado é identificado, conforme item 3.4;
2) As solicitações de revogação, bem como as ações delas decorrentes, realizadas pela ACSerpro-SRF e AR são registradas e armazenadas;
3) As justificativas para a revogação de um certificado são documentadas e arquivadas;
4) O processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contenha o certificado revogado.

O prazo máximo para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação pela ACSerpro-SRF, é de uma hora.

A ACSerpro-SRF responde plenamente por todos os danos causados pelo uso de um certificado no período compreendido entre a solicitação de sua revogação e a emissão da correspondente LCR.

4.4.4 Prazo para solicitação de revogação

Os Titulares de Certificados ou as entidades descritas no item 4.4.2 devem fazer a solicitação de revogação imediatamente quando configuradas as circunstâncias definidas no item 4.4.1.

A ACSerpro-SRF não estabelece prazo para aceitação de certificado uma vez que a solicitação de revogação do mesmo poderá ser feita a qualquer momento sem a cobrança de tarifa.

4.4.5 Circunstâncias para suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

4.4.6 Quem pode solicitar suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

4.4.7 Procedimento para solicitação de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

4.4.8 Limites no período de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

4.4.9 Freqüência de emissão de LCR

A Lista de Certificados Revogados (LCR) da ACSerpro-SRF é atualizada em sua entrada a cada 1 hora.

Os números de série de certificados de qualquer entidade final que estejam revogados aparecem na LCR emitida pela ACSerpro-SRF. Estes números permanecem nas LCR emitidas até a data de expiração dos certificados ser atingida, sendo removidos na primeira LCR emitida após data de suas expirações.

São emitidas LCR na freqüência determinada neste item, mesmo quando não houver nenhuma mudança ou atualização, para assegurar a periodicidade da informação.

4.4.10 Requisitos para verificação de LCR

Todos os certificados revogados são listados na LCR que pode ser acessada na página da ACSerpro-SRF ou no endereço URL contido no próprio certificado.

Antes de aceitar um certificado, Usuários de Certificados (partes confiáveis) devem verificar a situação do mesmo na LCR corrente. Se for utilizada uma cópia local da LCR, esta deve ser atualizada se tiver sido gerada há mais de 24 horas. Também deve ser verificada a autenticidade da LCR por meio das verificações de assinatura e do seu período de validade. Os Usuários devem utilizar aplicações cliente que atendam a estas especificações.

4.4.11 Disponibilidade para revogação/verificação de estado de certificado *on-line*

A ACSerpro-SRF não suporta os processos de revogação ou verificação da situação de estado de certificados de forma *on-line*.

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

A ACSerpro-SRF não suporta os processos de revogação de forma *on-line*.

4.4.13 Outras formas disponíveis para divulgação de revogação

A ACSerpro-SRF não suporta outras formas para divulgação da revogação que não através da publicação de LCR.

4.4.14 Requisitos para verificação de outras formas de divulgação de revogação

A ACSerpro-SRF não suporta qualquer outra forma de verificação de situação de certificados que não seja a consulta à LCR.

4.4.15 Requisitos especiais para o caso de comprometimento de chave

Todas as ocorrências de comprometimento ou suspeita de comprometimento de chaves devem ser submetidas à AR por escrito e, a solicitação da revogação deve ser imediatamente feita com base nos procedimentos descritos no item 3.4. O relato deve incluir o nome do Titular do Certificado e as circunstâncias sob a qual o comprometimento ocorreu.

A AR da ACSerpro-SRF irá investigar todos os relatos e tomar as ações apropriadas. Os resultados destas investigações e ações tomadas são registrados juntamente com o relato do Titular e arquivados pela AR.

4.5 Procedimentos de Auditoria de Segurança

Os itens a seguir estão definidos na DPC ACSerpro-SRF sob a mesma numeração. O leitor deve obter a cópia atualizada da DPC da ACSerpro-SRF e referir-se ao item de mesmo número.

4.5.1 Tipos de eventos registrados

Vide item de mesmo número na DPC da ACSerpro-SRF.

4.5.2 Freqüência de auditoria de registros (*logs*)

Vide item de mesmo número na DPC da ACSerpro-SRF.

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

Vide item de mesmo número na DPC da ACSerpro-SRF.

4.5.4 Proteção de registro (*log*) de auditoria

Vide item de mesmo número na DPC da ACSerpro-SRF.

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

Vide item de mesmo número na DPC da ACSerpro-SRF.

4.5.6 Sistema de coleta de dados de auditoria

Vide item de mesmo número na DPC da ACSerpro-SRF.

4.5.7 Notificação de agentes causadores de eventos

Vide item de mesmo número na DPC da ACSerpro-SRF.

4.5.8 Avaliações de vulnerabilidade

Vide item de mesmo número na DPC da ACSerpro-SRF.

4.6 Arquivamento de Registros

Os itens a seguir estão definidos na DPC da ACSerpro-SRF sob a mesma numeração. O leitor deve obter a cópia atualizada da DPC e referir-se ao item de mesmo número.

4.6.1 Tipos de registros arquivados

Vide item de mesmo número na DPC da ACSerpro-SRF.

4.6.2 Período de retenção para arquivo

Vide item de mesmo número na DPC da ACSerpro-SRF.

4.6.3 Proteção de arquivo

Vide item de mesmo número na DPC da ACSerpro-SRF.

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

Vide item de mesmo número na DPC da ACSerpro-SRF.

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

Vide item de mesmo número na DPC da ACSerpro-SRF.

4.6.6 Sistema de coleta de dados de arquivo

Vide item de mesmo número na DPC da ACSerpro-SRF.

4.6.7 Procedimentos para obter e verificar informação de arquivo

Vide item de mesmo número na DPC da ACSerpro-SRF.

4.7 Troca de chave

Os certificados emitidos pela ACSerpro-SRF, e as respectivas chaves criptográficas geradas por seus Titulares, possuem prazo de validade de 3 (três) anos a partir do momento da aprovação do certificado. Antes da expiração deste prazo, novo par de chaves deve ser gerado pelo Titular e nova solicitação de certificados deverá ser efetuada à ACSerpro-SRF.

4.8 Comprometimento e Recuperação de Desastre

Os itens a seguir estão definidos na DPC da ACSerpro-SRF sob a mesma numeração. O leitor deve obter a cópia atualizada da DPC e referir-se ao item de mesmo número para informações sobre o processo de recuperação de desastre da ACSerpro-SRF.

4.8.1 Recursos computacionais, *software* ou dados são corrompidos

Vide item de mesmo número na DPC da ACSerpro-SRF.

4.8.2 Certificado de entidade é revogado

Vide item de mesmo número na DPC da ACSerpro-SRF.

4.8.3 Chave de entidade é comprometida

Vide item de mesmo número na DPC da ACSerpro-SRF.

4.8.4 Segurança dos recursos após desastre natural ou de outra natureza

Vide item de mesmo número na DPC da ACSerpro-SRF.

4.9 Extinção da ACSerpro-SRF

Vide item de mesmo número na DPC da ACSerpro-SRF.

5. Controles de Segurança Física, Procedimental e de Pessoas

Os itens a seguir estão definidos na DPC da ACSerpro-SRF sob a mesma numeração. O leitor deve obter a cópia atualizada da DPC e referir-se ao item de mesmo número para quaisquer informações sobre os controles de segurança física, procedimental e de pessoas no âmbito da ACSerpro-SRF.

5.1 Controles Físicos

5.1.1 Construção e localização das instalações

Vide item de mesmo número na DPC da ACSerpro-SRF.

5.1.2 Acesso físico

Vide item de mesmo número na DPC da ACSerpro-SRF.

5.1.3 Energia e ar condicionado

Vide item de mesmo número na DPC da ACSerpro-SRF.

5.1.4 Exposição à água

Vide item de mesmo número na DPC da ACSerpro-SRF.

5.1.5 Prevenção e proteção contra incêndio

Vide item de mesmo número na DPC da ACSerpro-SRF.

5.1.6 Armazenamento de mídia

Vide item de mesmo número na DPC da ACSerpro-SRF.

5.1.7 Destruição de lixo

Vide item de mesmo número na DPC da ACSerpro-SRF.

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

Vide item de mesmo número na DPC da ACSerpro-SRF.

5.2 Controles Procedimentais

5.2.1 Perfis qualificados

Vide item de mesmo número na DPC da ACSerpro-SRF.

5.2.2 Número de pessoas necessário por tarefa

Vide item de mesmo número na DPC da ACSerpro-SRF.

5.2.3 Identificação e autenticação para cada perfil

Vide item de mesmo número na DPC da ACSerpro-SRF.

5.3 Controles de Pessoal

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

Vide item de mesmo número na DPC da ACSerpro-SRF.

5.3.2 Procedimentos de verificação de antecedentes

Vide item de mesmo número na DPC da ACSerpro-SRF.

5.3.3 Requisitos de treinamento

Vide item de mesmo número na DPC da ACSerpro-SRF.

5.3.4 Freqüência e requisitos para reciclagem técnica

Vide item de mesmo número na DPC da ACSerpro-SRF.

5.3.5 Freqüência e seqüência de rodízio de cargos

Vide item de mesmo número na DPC da ACSerpro-SRF.

5.3.6 Sanções para ações não autorizadas

Vide item de mesmo número na DPC da ACSerpro-SRF.

5.3.7 Requisitos para contratação de pessoal

Vide item de mesmo número na DPC da ACSerpro-SRF.

5.3.8 Documentação fornecida ao pessoal

Vide item de mesmo número na DPC da ACSerpro-SRF.

6. Controles Técnicos de Segurança

Nos itens seguintes, são descritas as medidas de segurança necessárias para proteger as chaves criptográficas dos Titulares de Certificados emitidos segundo esta PC. Também são definidos outros controles técnicos de segurança utilizados pela ACSerpro-SRF 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

O par de chaves criptográficas e o certificado é gerado pelo próprio Titular do Certificado. Quando o titular do certificado for pessoa jurídica, esta indicará por seu(s) representante(s) legal(s), a pessoa responsável pela geração, utilizando para isto o cartão inteligente (*smartcard*) ou token.

A chave privada é gerada no cartão inteligente ou token e no mesmo permanece, não sendo utilizada ou transportada fora do mesmo.

Os dispositivos de armazenamento da chave asseguram, por meios técnicos e procedimentais adequados, que:

1) A chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;
2) A chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida. Esta chave é protegida por meio de tecnologias atualizadas;
3) A chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros;
4) A entrega do certificado somente ocorre ao detentor da chave privada correspondente à chave pública constante do certificado.

Ao ser gerada, a chave privada da entidade titular deverá ser gravada cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, no meio de armazenamento definido para o tipo de certificado A3.

A chave privada deverá trafegar cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e a mídia utilizada para o seu armazenamento.

Esse meio de armazenamento não modifica os dados a serem assinados nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura. O tipo de certificado adotado na ACSerpro-SRF e descrito nesta PC é o A3.

6.1.2 Entrega da chave privada à entidade titular

Item não aplicável uma vez que é o próprio Titular que gera seu par de chaves.

6.1.3 Entrega da chave pública para o emissor de certificado

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

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

O certificado da ACSerpro-SRF e demais certificados de sua cadeia de certificação são disponibilizados, para todos usuários da ACSerpro-SRF, segundo as formas abaixo:

1) Formato PKCS#7 (RFC 2315), que inclui toda a cadeia de certificação, no momento da disponibilização de um certificado para seu Titular;
2) Página *Web* da ACSerpro-SRF.

6.1.5 Tamanhos de chave

O tipo de certificado emitido sob esta PC pela ACSerpro-SRF é o A3, que exige para o tamanho das chaves de seus certificados o mínimo de 1024 bits.

6.1.6 Geração de parâmetros de chaves assimétricas

Os Titulares de certificados devem garantir que os parâmetros de geração do seu par de chaves assimétricas, relativo ao certificado emitido sob esta PC pela ACSerpro-SRF, seguem o padrão FIPS (*Federal Information Processing Standards*) 140-1.
O CSP (*Cryptographic Service Provider*) que será utilizado para esta finalidade poderá ser validado, quanto ao padrao FIPS 140 level 1, no seguinte endereço: http://csrc.nist.gov/cryptval/140-1.htm, através de um arquivo disponibilizado para download contendo os módulos criptográficos certificados pelos laboratórios credenciados pelo NIST.

6.1.7 Verificação da qualidade dos parâmetros

A qualidade dos parâmetros pode ser verificada de acordo com as normas estabelecidas pelo CMVP (*Cryptographic Module Validation Program*) do NIST (*National Institute of Standards and Technology*) uma vez que este é o programa que determina as normas para validação do padrao FIPS 140 level 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 hardware, cartão inteligente ou token com capacidade de processamento, conforme previsto pela ICP-Brasil

Esta PC caracteriza o processo utilizado para a geração de chaves criptográficas dos Titulares de Certificados, com base nos requisitos aplicáveis estabelecidos pelo documento “Requisitos Mínimos para Políticas de Certificados na ICP-Brasil”.

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

As chaves privadas dos Titulares de Certificados emitidos pela ACSerpro-SRF serão utilizadas conforme descrito no item 1.3.4.1.

6.2 Proteção da Chave Privada

Nos itens seguintes são definidos os requisitos para a proteção das chaves privadas dos Titulares de Certificados emitidos segundo a PC.

6.2.1 Padrões para módulo criptográfico

Os Titulares de Certificado devem garantir que o módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão FIPS (*Federal Information Processing Standards*) 140-1 – requerido pela ACSerpro-SRF para os certificados emitidos sob esta PC.

O CSP (*Cryptographic Service Provider*) que será utilizado para esta finalidade poderá ser validado, quanto ao padrao FIPS 140 level 1, no seguinte endereço: http://csrc.nist.gov/cryptval/140-1.htm, através de um arquivo disponibilizado para download contendo os módulos criptográficos certificados pelos laboratórios credenciados pelo NIST.

6.2.2 Controle “n de m” para chave privada

Item não aplicável.

6.2.3 Recuperação (*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

A ACSerpro-SRF não mantém a cópia da chave privada do certificado tipo A3, emitidos sob desta PC.

Titulares de Certificado também não possuem cópia de segurança de suas chaves criptográficas, uma vez que o cartão inteligente ou token utilizado não permite que a chave privada seja exportada.

6.2.5 Arquivamento de chave privada

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

6.2.6 Inserção de chave privada em módulo criptográfico

Item não aplicável, uma vez que a chave é gerada dentro do próprio módulo.

6.2.7 Método de ativação de chave privada

A chave privada, gerada em cartão inteligente ou token, é ativada mediante senha solicitada pelo CSP (*Cryptographic Service Provider*) do fornecedor do próprio cartão inteligente ou token. Os critérios para escolha da senha devem obedecer aos descritos no item 2.8 desta PC. A senha deve ser criada e mantida apenas pelo Titular do Certificado, sendo para seu uso e conhecimento exclusivo.

Ao receber o cartão ou token pela primeira vez, a senha deve ser criada e modificada antes da geração do par de chaves.

Os Titulares de Certificados podem alterar suas senhas a qualquer momento, sendo recomendável que o façam no mínimo a cada 3 meses.

6.2.8 Método de desativação de chave privada

A desativação da chave privada ocorre em função da expiração ou em função da revogação do certificado digital correspondente.

A eliminação das chaves criptográficas do cartão inteligente ou token deve ser feita pelo próprio Titular do Certificado através de opção disponível no *software* de gerenciamento fornecido do dispositivo.

6.2.9 Método de destruição de chave privada

A eliminação das chaves do dispositivo de armazenamento deve ser feita pelo próprio Titular do Certificado através de opção disponível no *software* de gerenciamento fornecido junto com o dispositivo.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

A ACSerpro-SRF armazena os certificados contendo as chaves públicas dos Titulares de Certificados de assinatura digital por ela emitidos, após a expiração dos certificados correspondentes, por 30 (trinta) anos, na forma da legislação em vigor, para verificação de assinaturas geradas durante seu prazo de validade.

6.3.2 Períodos de uso para as chaves pública e privada

As chaves privadas dos respectivos Titulares deverão ser 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, que é de 3 anos para o certificado do tipo A3, emitido sob esta PC.

6.4 Dados de Ativação

A ACSerpro-SRF não gera dados de ativação.

6.4.1 Geração e instalação dos dados de ativação

Item não aplicável.

6.4.2 Proteção dos dados de ativação

Item não aplicável.

6.4.3 Outros aspectos dos dados de ativação

Item não aplicável.

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

Os equipamentos onde são gerados os pares de chaves criptográficas dos Titulares de Certificados devem dispor de mecanismos mínimos que garantam a segurança computacional. O equipamento onde serão gerados os pares de chaves criptográficas possui conexão como dispositivo de mídia inteligente e o respectivo driver instalado. A mídia inteligente possui processador criptográfico com capacidade de geração interna das chaves e suas características obedecem às especificações da norma ISO 7816.

6.5.2 Classificação da segurança computacional

Item não aplicável.

6.6 Controles Técnicos do Ciclo de Vida

Item não aplicável pois a ACSerpro-SRF não exige um *software* específico para a utilização dos certificados emitidos segundo esta PC.

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 FIPS (*Federal Information Processing Standards*) 140-1 – requerido pela ACSerpro-SRF para os certificados emitidos sob esta PC.

O CSP (*Cryptographic Service Provider*) que será utilizado para esta finalidade poderá ser validado, quanto ao padrao FIPS 140 level 1, no seguinte endereço: *http://csrc.nist.gov/cryptval/140-1.htm*, através de um arquivo disponibilizado para download contendo os módulos criptográficos certificados pelos laboratórios credenciados pelo NIST.

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 ACSerpro-SRF, segundo esta PC, estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8, especificado pelo CG da ICP-Brasil.

7.1.1 Número de versão

Todos os certificados emitidos pela ACSerpro-SRF, segundo esta PC, implementam a versão 3 de certificado definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 2459.

7.1.2 Extensões de certificado

A ACSerpro-SRF implementa para os certificados emitidos segundo esta PC as seguintes extensões definidas como obrigatórias pela ICP-Brasil:

1. "*Authority Key Identifier*", não crítica: o campo **keyIdentifier** contém o resumo SHA-1 da chave pública da ACSerpro-SRF;
2. "*Key Usage*", crítica: somente os bits **digitalSignature**, **nonRepudiation** e **keyEncipherment** são ativados;
3. "*Certificate Policies*", não crítica: contém o OID desta PC e o endereço *URL* da página *Web* da ACSerpro-SRF (https://ccd.serpro.gov.br/acserprosrf/docs/dpcacserprosrf.pdf), definida no item 2.6.1, com a DPC da ACSerpro-SRF;
4. "*CRL Distribution Points*", não crítica: contém o endereço *URL* da página *Web,* (http://ccd.serpro.gov.br/lcr/acserprosrf.crl) definida no item 2.6.1, onde se obtém a LCR da ACSerpro-SRF para os certificados emitidos segundo esta PC;
5. "*Subject Alternative Name*", não crítica e com os seguintes formatos para certificados:

Para certificados **e-CPF** os seguintes OtherName:

- 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 subseqüentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subseqüentes, o Número de Identificação Social-NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subseqüentes, o número do Registro Geral (RG) do titular; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva unidade da federação.

- 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 subseqüentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 posições subseqüentes, o município e a UF do Título de Eleitor.

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

- OID = 1.3.6.1.4.1.311.20.2.3 e conteúdo = Campo "Autenticação" que contém o domínio de login em estações de trabalho (UDN).

Para os certificados **e-CNPJ**, de equipamentos e aplicações os seguintes OtherName:

- 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 Registro Geral (RG) do responsável; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva unidade da federação;

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

- OID = 2.16.76.1.3.3 e conteúdo = Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica;

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

A ACSerpro-SRF implementa também, para os certificados e-CPF e e-CNPJ emitidos sob esta PC:

- a sub-extensão "*rfc822Name*", parte da extensão obrigatória "*Subject Alternative Name*", contendo o endereço e-mail do titular do certificado.
- a extensão "*Extended-key-usage*" contendo os valores "*client authentication*" (OID 1.3.6.1.5.5.7.3.2), "*E-mail protection*" (OID 1.3.6.1.5.5.7.3.4) e "Smart Card Logon" (OID 1.3.6.1.4.1.311.20.2.2).

O conjunto de informações definido em cada campo otherName é armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING, com exceção do campo OtherName UDN cuja cadeia de caracteres é do tipo UTF-8 String.

Para o correto preenchimento dos campos *othername* deve ser observado o seguinte:

- Para os certificados e-CPF, os campos CPF, Data de Nascimento, Título de Eleitor são obrigatórios.
- Para os certificados e-CNPJ, os campos CPF, data de nascimento do responsável e o CNPJ da empresa, são obrigatórios.
- Se o número do RG, NIS (PIS, PASEP ou CI) ou CEI não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero" .

- Se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF.
- As 6 (seis) 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.
- O preenchimento do campo "Autenticação" é opcional, e apenas os caracteres de A a Z, de 0 a 9, "-" (hifem), "@" (arroba), "." (ponto) são aceitos.
- Para todos os campos OtherName, exceto o campo "Autenticação", 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.
- Outros campos que compõem a extensão "Subject Alternative Name" poderão ser utilizados, na forma e com os propósitos definidos na RFC 2459".

7.1.3 Identificadores de algoritmo

O OID (*Object Identifiers*) do algoritmo criptográfico utilizado pela ACSerpro-SRF e admitido no âmbito da ICP-Brasil é o seguinte: SHA-1[1] com RSA, OID = 1.2.840.113549.1.1.5.

7.1.4 Formatos de nome

Certificados e-CPF

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=Secretaria da Receita Federal-SRF
OU=SRF e-CPF A3
OU= <Entidade Aprovadora do Certificado>
CN = *<Nome do titular do certificado>:99999999999*

Onde "99999999999" é o CPF do Titular do Certificado

Certificados e-CNPJ

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=Secretaria da Receita Federal-SRF
OU=SRF e-CNPJ A3
OU=<Entidade aprovadora do Certificado>
S= *<Sigla da Unidade da Federação>*
L = *<Cidade>*
CN = *<Nome Empresarial>:99999999999999*

[1] A função *hash* SHA-1 está descrita em FIPS 180-1.

Onde "*99999999999999*" é o CNPJ da pessoa jurídica.

7.1.5 Restrições de nome

São as seguintes as restrições aplicáveis para os nomes dos Titulares de Certificados no âmbito da ACSerpro-SRF:

1) não deverão ser utilizados sinais de acentuação, tremas ou cedilhas;
2) 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: 2.16.76.1.2.3.4

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 ACSerpro-SRF, (https://ccd.serpro.gov.br/acserprosrf/docs/dpcacserprosrf.pdf).

7.1.9 Semântica de processamento para extensões críticas

Extensões críticas devem ser interpretadas conforme a RFC 2459.

7.2 Perfil de LCR

7.2.1 Número de versão

As LCR geradas pela ACSerpro-SRF, segundo esta PC, implementam a versão 2 de LCR definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 2459.

7.2.2 Extensões de LCR e de suas entradas

A ACSerpro-SRF adota as seguintes extensões de LCR previstas pela ICP-Brasil:

1) "*Authority Key Identifier*": contém o resumo SHA-1 da chave pública da ACSerpro-SRF.
2) "*CRL Number*", não crítica: contém número seqüencial para cada LCR emitida.

8. Administração de Especificação

Os itens seguintes definem como será mantida e administrada esta PC.

8.1 Procedimentos de mudança de especificação

As alterações nas especificações desta PC são realizadas pela ACSerpro-SRF. Quaisquer modificações são submetidas à aprovação da AC-SRF, que por sua vez submeterá ao do CG da ICP-Brasil.

8.2 Políticas de publicação e notificação

A cada nova versão, esta PC é publicada na página *Web* da ACSerpro-SRF.

8.3 Procedimentos de aprovação

Esta PC foi submetida à aprovação da AC-SRF, que por sua vez submeteu ao CG da ICP-Brasil, durante o processo de credenciamento da ACSerpro-SRF, 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 ACSerpro-SRF.