Autoridade Certificadora

SOLUTI-JUS

Política de Certificado A3

(PC A3 da AC SOLUTI-JUS)

OID 2.16.76.1.2.3.46

Versão 1.1 de 7 de novembro de 2016

Classificação: Ostensivo

www.acsoluti.com.br

Sumário

Controle de Versão

Versão	Data	Descrição
1.1	07/11/2016	Adequação à versão 6.1 do DOC-ICP-04 (itens modificados: 1.1.8, 1.3.5.7, 6.1.1.1.1, 7.1.2.3, 7.1.2.4, 7.1.2.7, 7.1.2.8). Utilização da extensão SubjectAlternativeName (item 7.1.2.6). Utilização da extensão ExtendedKeyUsage (item 7.1.2.9 e 7.1.2.9.1). Remoção da extensão AIA na LCR (item 7.2.2). Dados de contato (item 1.4).
1.0	01/11/2012	Versão inicial, a partir do DOC-ICP-04 versão 5.1.

Tabela de Siglas

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AGR	Agente de Registro
AR	Autoridade 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 Pessoa Jurídica
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	Instrusion Detection System
IEC	International Eletrotechnical Commission
ISO	International Organization for Standardization
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecummunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social

SIGLA	DESCRIÇÃO
NIST	National Institutute of Satandards and Technology
OCSP	On-line Certificate Status Protocol
OID	Object Identifer
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	Proof of Pessession
PS	Política de Segurança
PSS	Prestadores de Serviço de Suporte
RIC	Registro de Identificação Civil
RFC	Request For Comments
RG	Registro Geral
SINRIC	Sistema Nacional de Registro de Identificação Civil
SNMP	Simpe Network Management Protocol
TCSEC	Trusted System Evaluation Criteria
TSDM	Trusted Software Development Methodology
UF	Unidade da Federação
URL	Uniform Resource Locator

1 INTRODUÇÃO

1.1 Visão Geral

1.1.1

Este documento descreve as políticas a serem obrigatoriamente observadas pela AC SOLUTI-JUS, integrante da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, na emissão de certificados de assinatura digital do tipo A3.

1.1.2

A PC AC SOLUTI-JUS A3 elaborada no âmbito da ICP-Brasil adota obrigatoriamente a estrutura dos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL[1].

1.1.3

Não se aplica.

1.1.4

Não se aplica.

1.1.5

Certificados do tipo A3, de assinatura, podem, conforme a necessidade, ser emitidos pela AC SOLUTI-JUS para pessoas físicas, pessoas jurídicas, equipamentos, aplicações ou assinatura de código.

1.1.6

Não se aplica.

1.1.7

Não se aplica.

1.1.8

Não se aplica.

1.2 Identificação

1.2.1

Este documento é chamado Política de Certificado de Assinatura Digital, Tipo A3, da AC SOLUTI-JUS, ou simplesmente **PC A3 da AC SOLUTI-JUS**.

1.2.2

O OID desta PC é 2.16.76.1.2.3.46.

1.3 Comunidade e Aplicabilidade

Nos itens seguintes são referidos os itens correspondentes da DPC AC SOLUTI-JUS. Apenas aspectos específicos desta PC serão descritos, quando for o caso.

1.3.1 Autoridades Certificadoras

1.3.1.1

Esta PC refere-se à Autoridade Certificadora SOLUTI-JUS (AC SOLUTI-JUS), integrante da ICP-Brasil, sob a hierarquia da AC-JUS e da AC Raiz.

1.3.1.2

As práticas de certificação da AC SOLUTI-JUS estão descritas na DPC AC SOLUTI-JUS.

1.3.2 Autoridades de Registro

1.3.2.1

O endereço da página web (URL) da AC SOLUTI-JUS é **http://ccd.acsoluti.com.br/**, onde estarão publicados os dados abaixo, referentes às 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 se descredenciado da cadeia da AC, com 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 ARs vinculadas com outras ARs da ICP-Brasil, se for o caso.

1.3.2.2

A AC SOLUTI-JUS mantém as informações acima atualizadas.

1.3.3 Prestador de Serviço de Suporte

1.3.3.1 Identificação

A relação de todos os Prestadores de Serviço de Suporte – PSS – vinculados diretamente à AC SOLUTI-JUS e/ou por intermédio de suas ARs é publicada em sua página web (**http://ccd.acsoluti.com.br/**).

1.3.3.2 Definição e classificação

PSS são entidades utilizadas pela AC e/ou suas ARs para desempenhar as atividades descritas nesta DPC ou nas PCs e são classificadas de acordo com o tipo de atividade prestada:

a) disponibilização de infraestrutura física e lógica;

b) disponibilização de recursos humanos especializados; ou

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

1.3.3.3

A AC SOLUTI-JUS mantém as informações acima atualizadas.

1.3.4 Titulares de Certificado

Os Titulares de Certificados desta PC A3 da AC SOLUTI-JUS são pessoas físicas ou jurídicas autorizadas pela AR vinculada a receber um certificado digital para sua própria utilização.

Os certificados emitidos pela AC SOLUTI-JUS, sob a hierarquia da AC-JUS, são denominados **Cert-JUS** e destinam-se aos órgãos da administração pública direta e indireta e identificam seus titulares relacionando-os a determinado órgão público. Cada órgão público que desejar fazer uso de certificados **Cert-JUS** é responsável pelas informações funcionais e institucionais constantes no certificado digital. Órgãos não pertencentes ao Poder Judiciário deverão solicitar cadastramento junto à AC-JUS.

Para a emissão de qualquer certificado Cert-JUS pela AC SOLUTI-JUS é necessária AUTORIZAÇÃO da autoridade competente da instituição à qual o certificado está relacionado.

Para o disposto neste documento, entende-se como autoridade competente: a autoridade máxima do órgão; o representante legal do órgão; outra pessoa expressamente designada para esta finalidade, por meio de documento oficial.

O titular de certificado emitido pela AC SOLUTI-JUS para Equipamento Servidor e Código Seguro será sempre um órgão público e o responsável pelo certificado deverá ser, obrigatoriamente, servidor público, indicado e autorizado pela autoridade competente.

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

A AC SOLUTI-JUS leva em conta o nível de segurança previsto para o certificado definido por esta PC na

definição das aplicações para o certificado. Esse nível de segurança é caracterizado pelos requisitos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, frequência de emissão da correspondente Lista de Certificados Revogados – LCR e extensão do período de validade do certificado.

1.3.5.4

Os certificados de tipo A3 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.

1.3.5.7

Não se aplica.

1.4 Dados de Contato

SOLUTI – Certificação Digital
Avenida 136, nº 797, Edifício New York Square, Sala 1901-B, Setor Sul
74.093-250 – Goiânia – Goiás
Telefones: (62) 3412-0200 / 3999-6000
E-mail: acsoluti@acsoluti.com.br
A/C: Vinicius Vieira de Sousa

2 DISPOSIÇÕES GERAIS

Nos itens seguintes são referidos os itens correspondentes da DPC AC SOLUTI-JUS. Apenas aspectos específicos desta PC serão descritos, quando for o caso.

2.1 Obrigações e Direitos

2.1.1 Obrigações da AC SOLUTI-JUS

2.1.2 Obrigações das ARs

2.1.3 Obrigações do Titular do Certificado

2.1.4 Direitos da Terceira Parte (Relying Party)

2.1.5 Obrigações do Repositório

2.2 Responsabilidades

2.2.1 Responsabilidades da AC SOLUTI-JUS

2.2.2 Responsabilidades da AR

2.3 Responsabilidade Financeira

2.3.1 Indenizações devidas pela terceira parte usuária (Relying Party)

2.3.2 Relações Fiduciárias

2.3.3 Processos Administrativos

2.4 Interpretação e Execução

2.4.1 Legislação

2.4.2 Forma de interpretação e notificação

2.4.3 Procedimentos de solução de disputa

2.5 Tarifas de Serviço

2.5.1 Tarifas de emissão e renovação de certificados

Nos itens seguintes são referidos os itens correspondentes da DPC AC SOLUTI-JUS. Apenas aspectos específicos desta PC serão descritos, quando for o caso.

3.4 Solicitação de Revogação

4 REQUISITOS OPERACIONAIS

Nos itens seguintes são referidos os itens correspondentes da DPC AC SOLUTI-JUS. Apenas aspectos específicos desta PC serão descritos, quando for o caso.

4.1 Solicitação de Certificado

4.2 Emissão de Certificado

4.3 Aceitação de Certificado

4.4 Suspensão e Revogação de Certificado

4.4.1 Circunstâncias para revogação

4.4.2 Quem pode solicitar revogação

4.4.3 Procedimento para solicitação de revogação

4.4.4 Prazo para solicitação de revogação

4.4.5 Circunstâncias para suspensão

4.4.6 Quem pode solicitar suspensão

4.4.7 Procedimento para solicitação de suspensão

4.4.8 Limites no período de suspensão

4.4.9 Frequência de emissão de LCR

4.4.10 Requisitos para verificação de LCR

4.4.11 Disponibilidade para revogação/verificação de status on-line

4.4.12 Requisitos para verificação de revogação on-line

4.4.13 Outras formas disponíveis para divulgação de revogação

4.4.14 Requisitos para verificação de outras formas de divulgação de revogação

4.4.15 Requisitos especiais para o caso de comprometimento de chave

4.5 Procedimentos de Auditoria de Segurança

4.5.1 Tipos de Evento Registrados

4.5.2 Frequência de auditoria de registros (logs)

4.5.3 Período de Retenção para registros (logs) de Auditoria

4.5.4 Proteção de registro (log) de Auditoria

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

4.5.6 Sistema de coleta de dados de auditoria

4.5.7 Notificação de agentes causadores de eventos

4.5.8 Avaliações de vulnerabilidade

4.6 Arquivamento de Registros

4.6.1 Tipos de registros arquivados

4.6.2 Período de retenção para arquivo

4.6.3 Proteção de arquivos

4.6.4 Procedimentos para cópia de segurança (backup) de arquivos

Nos itens seguintes são referidos os itens correspondentes da DPC AC SOLUTI-JUS. Apenas aspectos específicos desta PC serão descritos, quando for o caso.

6 CONTROLES TÉCNICOS DE SEGURANÇA

6.1 Geração e Instalação do Par de Chaves

6.1.1 Geração do par de chaves

6.1.1.1

Quando o titular de certificado for uma pessoa física, esta será responsável pela geração do par de chaves criptográficas. Quando o titular de certificado for órgão ou entidade, este indicará, por seu(s) representante(s) legal(is), a pessoa responsável pela geração do par de chaves criptográficas e pelo uso do Certificado.

6.1.1.1.1

Não se aplica.

6.1.1.2

O par de chaves criptográficos relativos aos certificados estabelecidos por esta PC é gerado pelo próprio Titular do Certificado, respeitando os seguintes critérios:

a) A geração da chave privada ocorre em hardware criptográfico aprovado pelo CG da ICP-Brasil.

b) A entrega do certificado somente ocorre ao detentor da chave privada correspondente à chave pública constante do certificado.

6.1.1.3

O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados será o RSA, como 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 ICP-BRASIL[1], no meio de armazenamento definido para certificados do tipo A3, 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 de chave privada assegura, 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

A mídia de armazenamento da chave privada não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura. Seu repositório é protegido por senha e cifrado por hardware definido acima. O tipo de certificado emitido pela AC SOLUTI-JUS e descrito nesta PC é o A3.

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 AC SOLUTI-JUS por meio de uma troca on-line utilizando funções automáticas do software de certificação da AC SOLUTI-JUS. 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 AC SOLUTI-JUS, compreendem:

a) No momento da disponibilização de um certificado para seu titular, será utilizado o formato PKCS#7, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP BRASIL[1];

b) Página web da AC SOLUTI-JUS (http://ccd.acsoluti.com.br/);

c) Outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5 Tamanhos de chave

6.1.5.1

O tamanho das chaves criptográficas associadas aos certificados emitidos sob esta PC é de 2048 bits.

6.1.5.2

Os algoritmos e o tamanho das chaves utilizados nos diferentes tipos de certificados da ICP-Brasil estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

6.1.6 Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas dos Titulares de certificado adotam o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

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 hardware criptográfico aprovado pelo CG da 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 AC SOLUTI-JUS serão utilizadas conforme descrito no item 1.3.5. Para tanto, os certificados tem ativados os bits **digitalSignature**, **nonRepudiation** e **keyEncipherment**.

6.2 Proteção da Chave Privada

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 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

O titular do certificado poderá, a seu critério, manter cópia de segurança de sua chave privada.

6.2.4.2

A AC SOLUTI-JUS, responsável por essa 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 ICPBRASIL[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

Não se aplica.

6.2.7 Método de ativação de chave privada

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

Recomenda-se que a chave privada seja protegida por senha e que para sua ativação seja solicitada essa senha, que deve ser criada e mantida apenas pelo Titular do Certificado, sendo para seu uso e conhecimento exclusivo. É recomendável também que a senha seja alterada periodicamente.

6.2.8 Método de desativação de chave privada

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

6.2.9 Método de destruição de chave privada

A eliminação da chave da mídia armazenadora do certificado pode ser feita através do mesmo componente criptográfico utilizado para geração do par de chaves, que oferece opção que permite apagar a chave privada. O titular pode definir procedimentos necessários para destruição de sua chave privada.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

A AC SOLUTI-JUS prevê que as chaves públicas de titulares dos certificados de assinatura digital e as LCRs serão armazenadas pela própria AC SOLUTI-JUS, 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 A3 previstos nesta PC têm validade máxima de **3 (três) anos**.

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

É responsabilidade do Titular do Certificado garantir que os equipamentos onde são gerados os pares de chaves criptográficas dispõem de mecanismos mínimos que garantam a segurança computacional, como, por exemplo, proteção do equipamento com senha, proteção antivírus e criptografia para armazenamento da chave privada.

6.5.2 Classificação da segurança computacional

Item não aplicável.

6.6 Controles Técnicos do Ciclo de Vida

6.6.1 Controles de desenvolvimento de sistema

Como descrito no item correspondente da DPC AC SOLUTI-JUS.

6.6.2 Controles de gerenciamento de segurança

Como descrito no item correspondente da DPC AC SOLUTI-JUS.

6.6.3 Classificações de segurança de ciclo de vida

Como descrito no item correspondente da DPC AC SOLUTI-JUS.

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 token ou cartão criptográfico utilizado na geração e utilização de suas chaves criptográficas passou pela Homologação ICP-Brasil, ou que o HSM utilizado na geração e utilização de suas chaves criptográficas passou pela Homologação ICP-Brasil NSH-2, como definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

7 PERFIS DE CERTIFICADO E LCR

7.1 Perfil do Certificado

Todos os certificados emitidos pela AC SOLUTI-JUS, segundo esta PC, estão em conformidade com o formato definido pelo padrão ITU X.509, especificado pelo CG da ICP-Brasil.

Também estão de acordo com o Leiaute dos Certificados Digitais Cert-JUS[1].

7.1.1 Número de versão

Todos os certificados emitidos pela AC SOLUTI-JUS, 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 descreve todas as extensões de certificado utilizadas e sua criticalidade.

7.1.2.2

Os certificados emitidos sob esta PC apresentam obrigatoriamente as seguintes extensões:

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

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

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

1. o campo **policyIdentifier** contém o OID desta PC: 2.16.76.1.2.3.46; e
2. o campo **policyQualifiers** contém o endereço Web da DPC da AC SOLUTI-JUS: **`http://ccd.acsoluti.com.br/docs/dpc-ac-soluti-jus.pdf`**

1 Disponível no repositório da AC-JUS no link **http://www.acjus.jus.br/repositorio/Docs_dpc_ps/Leiaute_acjus_v5.0.pdf**

d) **CRL Distribution Points**, não crítica: contém o endereço Web onde se obtém a LCR da AC SOLUTI-JUS:

1. Para certificados na hierarquia da Autoridade Certificadora Raiz Brasileira V5:
   i. **http://ccd.acsoluti.com.br/lcr/ac-soluti-jus-v5.crl**
   ii. **http://ccd2.acsoluti.com.br/lcr/ac-soluti-jus-v5.crl**
2. Para certificados na hierarquia da Autoridade Certificadora Raiz Brasileira V2:
   i. **http://ccd.acsoluti.com.br/lcr/ac-soluti-jus-v1.crl**
   ii. **http://ccd2.acsoluti.com.br/lcr/ac-soluti-jus-v1.crl**
   iii. **http://repositorio.icpbrasil.gov.br/lcr/ACSOLUTI/ac-soluti-jus-v1.crl**

e) **Authority Information Access**, não crítica:

1. Para certificados na hierarquia da Autoridade Certificadora Raiz Brasileira V5:
   i. uma entrada contendo o método de acesso **id-ad-caIssuer**, contendo o URL para a recuperação da cadeia de certificação: **http://ccd.acsoluti.com.br/lcr/ac-soluti-jus-v5.p7b**
2. Para certificados na hierarquia da Autoridade Certificadora Raiz Brasileira V2:
   i. uma entrada contendo o método de acesso **id-ad-caIssuer**, contendo o URL para a recuperação da cadeia de certificação: **http://ccd.acsoluti.com.br/lcr/ac-soluti-jus-v1.p7b**

f) **basicConstraints**, não crítica: contém o campo **CA=False**.

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 pessoa física (**Cert-JUS Institucional** e **Cert-JUS Poder Público**):

i. Três campos otherName, **obrigatórios**, contendo:

1. OID = 2.16.76.1.3.1, e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subsequentes, o Número de Identificação Social - NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do Registro Geral - RG do titular; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF. O CPF e data de nascimento do responsável são de preenchimento **obrigatório**.
2. OID = 2.16.76.1.3.6, e conteúdo = nas 12 (doze) posições o número do Cadastro Especifico do INSS (CEI) da pessoa física titular do certificado.
3. OID = 2.16.76.1.3.5, e conteúdo = nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subsequentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subsequentes, o município e a UF do Título de Eleitor.

ii. Campo otherName, obrigatório, para certificados vinculados ao Documento RIC, contendo: OID = 2.16.76.1.3.9, e conteúdo = nas primeiras 11 (onze) posições, o número de Registro de Identidade Civil;

iii. Campo otherName, **opcional**, OID = 1.3.6.1.4.1.311.20.2.3 (UPN), contendo nome de login em estações de trabalho. Deve estar na forma <usuário>@<domínio>.

b) Para certificado de aplicação, de equipamento, ou de assinatura de código (**Cert-JUS Equipamento Servidor** e **Cert-JUS Código Seguro**), quatro campos otherName, obrigatórios:

1. OID = 2.16.76.1.3.8, e conteúdo = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, **obrigatório**;
2. 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, **obrigatório**;
3. OID = 2.16.76.1.3.2, e conteúdo = nome do responsável pelo certificado, **obrigatório**;

4. OID = 2.16.76.1.3.4, e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do RG do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF. O CPF e data de nascimento do responsável são de preenchimento **obrigatório**.

7.1.2.4

Os campos otherName definidos como obrigatórios pela ICP-Brasil estão de acordo com as seguintes especificações:

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

b) Quando os números de NIS (PIS, PASEP ou CI), RG, 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 ou Título de Eleitor, 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, observado o disposto no item 7.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais.

7.1.2.5

Não se aplica.

7.1.2.6

A AC SOLUTI-JUS pode implementar a extensão "**SubjectAlternativeName**", **não crítica**, definida como **opcional** pela ICP-Brasil, com os seguintes campos:

a) Certificados de pessoa física (**Cert-JUS Institucional** e **Cert-JUS Poder Público**):

i. Campo "**rfc822Name**" (OID= 2.5.29.17.1), **obrigatório**, contendo o e-mail institucional do titular do certificado. Este campo deverá estar no formato IA5string.

b) Certificados de assinatura de código (**Cert-JUS Código Seguro**):

i. Campo "**rfc822Name**" (OID= 2.5.29.17.1), **obrigatório**, contendo o e-mail institucional do responsável pelo certificado ou e-mail da unidade organizacional responsável pelo certificado. Este campo deverá estar no formato IA5string.

c) Certificados de aplicação ou de equipamento (**Cert-JUS Equipamento Servidor**):

i. Campo "**rfc822Name**" (OID= 2.5.29.17.1), **obrigatório**, contendo o e-mail institucional do responsável pelo certificado ou e-mail da unidade organizacional responsável pelo certificado. Este campo deverá estar no formato IA5string;

ii. Vários campos "dNSName" (OID 2.5.29.17.2), um para cada URL endereçada no certificado.

7.1.2.7

Não se aplica.

7.1.2.8

Não se aplica.

7.1.2.9

A AC SOLUTI-JUS pode implementar a extensão "**Extended-key-usage**", **não crítica**, definida como **opcional** pela ICP-Brasil, com os seguintes propósitos:

a) Certificados de pessoa física (**Cert-JUS Institucional** e **Cert-JUS Poder Público**):

i. "client authentication" OID = 1.3.6.1.5.5.7.3.2;

ii. "E-mail protection" OID = 1.3.6.1.5.5.7.3.4;

iii. "Smart Card Logon" OID = 1.3.6.1.4.1.311.20.2.2 (opcional);

b) Certificados de assinatura de código (**Cert-JUS Código Seguro**):

i. "code signing" OID = 1.3.6.1.5.5.7.3.3;

Certificados de assinatura de código não serão emitidos a partir de 01/01/2017.

c) Certificados de aplicação ou de equipamento (**Cert-JUS Equipamento Servidor**):

i. "server authentication" OID = 1.3.6.1.5.5.7.3.1;

ii. "client authentication" OID = 1.3.6.1.5.5.7.3.2 (opcional);

iii. Para serviço OCSP, somente "OCSPSigning" OID = 1.3.6.1.5.5.7.3.9;

Certificados de equipamento ou de aplicação não serão emitidos a partir de 01/01/2017.

7.1.2.9.1

O propósito "anyExtendedKeyUsage" OID = 2.5.29.37.0 não é utilizado na "Extended-key-usage".

7.1.3 Identificadores de algoritmo

O OID (Object Identifier) do algoritmo criptográfico utilizado para assinatura do certificado, pela AC SOLUTI-JUS , RSA com SHA-256, OID = 1.2.840.113549.1.1.11 é admitido no âmbito da ICP-Brasil, conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

7.1.4 Formatos de nome

7.1.4.1

O nome do titular do certificado, constante do campo "Subject", adota o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, das seguintes formas [2] [3]:

1. Para certificados na hierarquia da **Autoridade Certificadora Raiz Brasileira V5**:

a) Para certificado **Cert-JUS Institucional** [4]:

```
C = BR
O = ICP-Brasil
OU = Autoridade Certificadora da Justica – AC-JUS
OU = Cert-JUS Institucional - A3
OU = <Órgão de Lotação do Titular> <-> <Sigla>
OU = <Cargo do Titular>
CN = <Nome do Titular><:><#########>
```

b) Para certificado **Cert-JUS Poder Público** [5]:

```
C = BR
O = ICP-Brasil
OU = Autoridade Certificadora da Justica – AC-JUS
OU = Cert-JUS Poder Publico - A3
OU = <Órgão de Lotação do Titular> <-> <Sigla>
OU = <Cargo do Titular>
CN = <Nome do Titular><:><#########>
```

2 O tamanho máximo de cada componente do "Distinguished Name" (DN) é de 64 caracteres.
3 O nome e sigla do órgão deverão ser aquelas constantes da comunicação de cadastramento encaminhada pela AC-JUS.
4 No campo **CN**, pode ser escrito até o limite de 54 caracteres, vedada a abreviatura quando o nome do titular exceder esse limite. Os caracteres **"#"** representam os dígitos da matrícula do titular no órgão de lotação, e deve ter 9 (nove) caracteres ao todo. Se o número de matrícula tiver menos de nove caracteres, deve ser preenchido à direita com caracteres brancos (0x20 da NBR9611).
5 No campo **CN**, pode ser escrito até o limite de 54 caracteres, vedada a abreviatura quando o nome do titular exceder esse limite. Os caracteres **"#"** representam os dígitos da matrícula do titular no órgão de lotação, e deve ter 9 (nove) caracteres ao todo. Se o número de matrícula tiver menos de nove caracteres, deve ser preenchido à direita com caracteres brancos (0x20 da NBR9611).

2. Para certificados na hierarquia da **Autoridade Certificadora Raiz Brasileira V2**:

a) Para certificado **Cert-JUS Institucional** [6]:

```
C = BR
O = ICP-Brasil
OU = Autoridade Certificadora da Justica - AC-JUS
OU = Cert-JUS Institucional - A3
OU = <Órgão de Lotação do Titular> - <Sigla do Órgão>
OU = <Cargo do Titular>
CN = <Nome do titular>:<#########>
```

b) Para certificado **Cert-JUS Poder Público** [7]:

```
C = BR
O = ICP-Brasil
OU = Autoridade Certificadora da Justica - AC-JUS
OU = Cert-JUS Poder Público - A3
OU = <Órgão de Lotação do Titular> - <Sigla do Órgão>
OU = <Cargo do Titular>
CN = <Nome do titular>:<#########>
```

c) Para certificado **Cert-JUS Equipamento Servidor** [8]:

```
C = BR
O = ICP-Brasil
OU = Autoridade Certificadora da Justica - AC-JUS
OU = Cert-JUS Equipamento Servidor - A3
OU = <Órgão a que pertence> - <Sigla do Órgão>
OU = <Nome da unidade organizacional responsável pelo equipamento>
CN = <Nome DNS do equipamento ou nome da aplicação>
```

Certificados de equipamento ou de aplicação não serão emitidos a partir de 01/01/2017.

d) Para certificado **Cert-JUS Código Seguro** [9]:

```
C = BR
O = ICP-Brasil
OU = Autoridade Certificadora da Justica - AC-JUS
OU = Cert-JUS Codigo Seguro - A3
OU = <Nome da unidade organizacional responsável>
CN = <Nome do órgão constante do CNPJ>
```

Certificados de assinatura de código não serão emitidos a partir de 01/01/2017.

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

7.1.4.2

Não se aplica.

7.1.5 Restrições de nome

7.1.5.1

Não se aplica.

7.1.5.2

As restrições aplicáveis para os nomes dos titulares de certificado emitidos pela AC SOLUTI-JUS são as seguintes:

a) Não são admitidos sinais de acentuação, trema ou cedilhas;

i. caracteres acentuados devem ser substituídos por seu correspondente sem acento;

6 No campo **CN**, pode ser escrito até o limite de 54 caracteres, vedada a abreviatura quando o nome do titular exceder esse limite. Os caracteres **"#"** representam os dígitos da matrícula do titular no órgão de lotação, e deve ter 9 (nove) caracteres ao todo. Se o número de matrícula tiver menos de nove caracteres, deve ser preenchido à direita com caracteres brancos (0x20 da NBR9611).

7 No campo **CN**, pode ser escrito até o limite de 54 caracteres, vedada a abreviatura quando o nome do titular exceder esse limite. Os caracteres **"#"** representam os dígitos da matrícula do titular no órgão de lotação, e deve ter 9 (nove) caracteres ao todo. Se o número de matrícula tiver menos de nove caracteres, deve ser preenchido à direita com caracteres brancos (0x20 da NBR9611).

8 O **CN (Common Name)** deve conter a URL correspondente ao equipamento servidor, ou o nome da aplicação ou serviço, a que esse certificado se refere.

9 O **CN (Common Name)** deve conter a nome do órgão constante do CNPJ, escrito até o limite de 64 caracteres, vedada a abreviatura.

ii. o cedilha deve ser substituído pelo caractere 'c';

b) Apenas são admitidos sinais alfanuméricos e os caracteres especiais descritos na tabela abaixo:

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

7.1.6 OID (Object Identifier) de Política de Certificado

O OID atribuído à esta Política de Certificado é: 2.16.76.1.2.3.46.

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 seguinte endereço da página Web (URL), que aponta para a DPC da AC SOLUTI-JUS: **http://ccd.acsoluti.com.br/docs/dpc-ac-soluti-jus.pdf**

7.1.9 Semântica de processamento para extensões críticas

Extensões críticas são interpretadas conforme a RFC 5280.

7.2 Perfil de LCR

7.2.1 Número de versão

As LCR geradas pela AC SOLUTI-JUS, segundo esta 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

A AC SOLUTI-JUS adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

a) “Authority Key Identifier”, não crítica: contém o resumo SHA-1 da chave pública da AC SOLUTI-JUS;

b) “CRL Number”, não crítica: contém número sequencial para cada LCR emitida.

8 ADMINISTRAÇÃO DE ESPECIFICAÇÃO

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

8.1 Procedimentos de Mudança de Especificação

As alterações nas especificações desta PC são realizadas pela AC SOLUTI-JUS. Quaisquer modificações são submetidas à aprovação da AC-JUS, 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 AC SOLUTI-JUS: **http://ccd.acsoluti.com.br/**

8.3 Procedimentos de Aprovação

Esta PC foi submetida à aprovação da AC-JUS, que por sua vez submeteu ao CG da ICP-Brasil, durante o processo de credenciamento da AC SOLUTI-JUS, conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3]. Como parte desse processo, além da conformidade com os documentos definidos pela ICP-Brasil, deverá ser verificada a compatibilidade entre esta PC e a DPC da AC SOLUTI-JUS.

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

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