

**Política de Certificado de Assinatura Digital Tipo
A3
da Autoridade Certificadora Certisign para a
Justiça**

PC A3 da AC Certisign-JUS

Versão 5.2 - 30/01/2017

ÍNDICE

1. INTRODUÇÃO	7
1.1.VISÃO GERAL	7
1.2.IDENTIFICAÇÃO	7
1.3.COMUNIDADE E APLICABILIDADE	7
1.3.1.Autoridades Certificadoras	7
1.3.2.Autoridades de Registro	7
1.3.3. Prestador de Serviço de Suporte	8
1.3.4.Titulares de Certificado.....	8
1.3.5.Aplicabilidade.....	8
1.4.DADOS DE CONTATO.....	8
2. DISPOSIÇÕES GERAIS	9
2.1. OBRIGAÇÕES E DIREITOS	9
2.1.1. Obrigações da AC Certisign-JUS.....	9
2.1.2. Obrigações das AR.....	9
2.1.3. Obrigações do Titular do Certificado	9
2.1.4. Direitos da Terceira Parte (Relying Party).....	9
2.1.5. Obrigações do Repositório.....	9
2.2. RESPONSABILIDADES	9
2.2.1. Responsabilidades da AC Certisign-JUS	9
2.2.2. Responsabilidades das AR.....	9
2.3. RESPONSABILIDADE FINANCEIRA.....	9
2.3.1. Indenizações devidas pela terceira parte(Relying Party).....	9
2.3.2. Relações Fiduciárias	9
2.3.3. Processos Administrativos.....	9
2.4. INTERPRETAÇÃO E EXECUÇÃO	9
2.4.1. Legislação.....	9
2.4.2. Forma de interpretação e notificação	9
2.4.3. Procedimentos da solução de disputa	9
2.5. TARIFAS DE SERVIÇO	9
2.5.1. Tarifas de emissão e renovação de certificados	9
2.5.2. Tarifas de acesso ao certificado	9
2.5.3. Tarifas de revogação ou de acesso à informação de status	9
2.5.4. Tarifas para outros serviços.....	9
2.5.5. Política de reembolso	9
2.6. PUBLICAÇÃO E REPOSITÓRIO	9
2.6.1. Publicação de informação da AC Certisign-JUS	9
2.6.2. Frequência de publicação	9
2.6.3. Controles de acesso	9
2.6.4. Repositórios.....	9
2.7. FISCALIZAÇÃO E AUDITORIA DE CONFORMIDADE.....	9
2.8. SIGILO	9
2.8.1. Disposições gerais.....	9
2.8.2. Tipos de informações sigilosas.....	9
2.8.3. Tipos de informações não sigilosas	9
2.8.4. Divulgação de informação de revogação ou suspensão de certificado.....	9
2.8.5. Quebra de sigilo por motivos legais.....	9
2.8.6. Informações a terceiros.....	9
2.8.7. Divulgação por solicitação do Titular.....	9
2.8.8. Outras circunstâncias de divulgação de informação	9
2.9. DIREITOS DE PROPRIEDADE INTELECTUAL	9
3. IDENTIFICAÇÃO E AUTENTICAÇÃO	9
3.1. REGISTRO INICIAL	10

3.1.1.	Disposições Gerais	10
3.1.2.	Tipos de nomes	10
3.1.3.	Necessidade de nomes significativos	10
3.1.4.	Regras para interpretação de vários tipos de nomes	10
3.1.5.	Unicidade de nomes.....	10
3.1.6.	Procedimento para resolver disputa de nomes.....	10
3.1.7.	Reconhecimento, autenticação e papel de marcas registradas	10
3.1.8.	Método para comprovar a posse de chave privada	10
3.1.9.	Autenticação da identidade de um indivíduo.....	10
3.1.9.1.	Documentos para efeitos de identificação de um indivíduo	10
3.1.9.2.	Informações contidas no certificado emitido para um indivíduo	10
3.1.10.	Autenticação da identidade de uma organização	10
3.1.10.1.	Disposições Gerais	10
3.1.10.2.	Documentos para efeitos de identificação de uma organização.....	10
3.1.10.3.	Informações contidas no certificado emitido para uma organização	10
3.1.11.	Autenticação da identidade de equipamento ou aplicação	10
3.1.11.1.	Disposições Gerais	10
3.1.11.2.	Procedimentos para efeitos de identificação de um equipamento ou aplicação.....	10
3.1.11.3.	Informações contidas no certificado emitido para um equipamento ou aplicação.....	10
3.1.12.	Autenticação de identificação de equipamento para certificado CF-e-SAT.....	10
3.2.	GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL	10
3.3.	GERAÇÃO DE NOVO PAR DE CHAVES APÓS EXPIRAÇÃO OU REVOGAÇÃO.....	10
3.4.	SOLICITAÇÃO DE REVOGAÇÃO	10
4.	REQUISITOS OPERACIONAIS	10
4.1.	SOLICITAÇÃO DE CERTIFICADO	10
4.2.	EMIÇÃO DE CERTIFICADO	10
4.3.	ACEITAÇÃO DE CERTIFICADO.....	10
4.4.	SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO	10
4.4.1.	Circunstâncias para revogação.....	10
4.4.2.	Quem pode solicitar revogação.....	10
4.4.3.	Procedimento para solicitação de revogação	10
4.4.4.	Prazo para solicitação de revogação	10
4.4.5.	Circunstâncias para suspensão	10
4.4.6.	Quem pode solicitar suspensão	10
4.4.7.	Procedimento para solicitação de suspensão.....	10
4.4.8.	Limites no período de suspensão.....	10
4.4.9.	Frequência de emissão de LCR.....	10
4.4.10.	Requisitos para verificação de LCR.....	10
4.4.11.	Disponibilidade para revogação ou verificação de status on-line	11
4.4.12.	Requisitos para verificação de revogação on-line	11
4.4.13.	Outras formas disponíveis para divulgação de revogação	11
4.4.14.	Requisitos para verificação de outras formas de divulgação de revogação	11
4.4.15.	Requisitos especiais para o caso de comprometimento de chave.....	11
4.5.	PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA	11
4.5.1.	Tipos de eventos registrados	11
4.5.2.	Frequência de auditoria de registros (logs).....	11
4.5.3.	Período de retenção para registros (logs) de auditoria	11
4.5.4.	Proteção de registro (log) de auditoria.....	11
4.5.5.	Procedimentos para cópia de segurança (backup) de registro (log) de auditoria	11
4.5.6.	Sistema de coleta de dados de auditoria	11
4.5.7.	Notificação de agentes causadores de eventos.....	11
4.5.8.	Avaliações de vulnerabilidade.....	11
4.6.	ARQUIVAMENTO DE REGISTROS.....	11
4.6.1.	Tipos de registros arquivados	11
4.6.2.	Período de retenção para arquivo.....	11
4.6.3.	Proteção de arquivo	11

4.6.4.	Procedimentos para cópia de segurança (backup) de arquivo	11
4.6.5.	Requisitos para datação (time-stamping) de registros	11
4.6.6.	Sistema de coleta de dados de arquivo	11
4.6.7.	Procedimentos para obter e verificar informação de arquivo	11
4.7.	TROCA DE CHAVE	11
4.8.	COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE	11
4.8.1.	Recursos computacionais, software, e dados corrompidos	11
4.8.2.	Certificado de entidade é revogado	11
4.8.3.	Chave da entidade é comprometida	11
4.8.4.	Segurança dos recursos após desastre natural ou de outra natureza	11
4.8.5.	Atividades das Autoridades de Registro	11
4.9.	EXTINÇÃO DOS SERVIÇOS DE AC, AR OU PSS	11
5.	CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL	11
5.1.	CONTROLES FÍSICOS	11
5.1.1.	Construção e localização das instalações	11
5.1.2.	Acesso físico nas instalações de AC	11
5.1.2.1.	Níveis de acesso	11
5.1.2.2.	Sistemas físicos de detecção	11
5.1.2.3.	Sistema de controle de acesso	11
5.1.2.4.	Mecanismos de emergência	11
5.1.3.	Energia e ar condicionado nas instalações de AC	11
5.1.4.	Exposição à água nas instalações de AC	11
5.1.5.	Prevenção e proteção contra incêndio nas instalações de AC	11
5.1.6.	Armazenamento de mídia nas instalações de AC	11
5.1.7.	Destruição de lixo nas instalações de AC	12
5.1.8.	Instalações de segurança (backup) externas (off-site) para AC	12
5.1.9.	Instalações técnicas de AR	12
5.2.	CONTROLES PROCEDIMENTAIS	12
5.2.1.	Perfis qualificados	12
5.2.2.	Número de pessoas necessário por tarefa	12
5.2.3.	Identificação e autenticação para cada perfil	12
5.3.	CONTROLES DE PESSOAL	12
5.3.1.	Antecedentes, qualificação, experiência e requisitos de idoneidade	12
5.3.2.	Procedimentos de verificação de antecedentes	12
5.3.3.	Requisitos de treinamento	12
5.3.4.	Frequência e requisitos para reciclagem técnica	12
5.3.5.	Frequência e sequência de rodízio de cargos	12
5.3.6.	Sanções para ações não autorizadas	12
5.3.7.	Requisitos para contratação de pessoal	12
5.3.8.	Documentação fornecida ao pessoal	12
6.	CONTROLES TÉCNICOS DE SEGURANÇA	12
6.1.	GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES	12
6.1.1.	Geração do par de chaves	12
6.1.2.	Entrega da chave privada à entidade titular do certificado	13
6.1.3.	Entrega da chave pública para emissor de certificado	13
6.1.4.	Disponibilização de chave pública da AC para usuários	13
6.1.5.	Tamanhos de chave	13
6.1.6.	Geração de parâmetros de chaves assimétricas	13
6.1.7.	Verificação da qualidade dos parâmetros	13
6.1.8.	Geração de chave por hardware ou software	13
6.1.9.	Propósitos de uso de chave (conforme o campo "key usage" na X.509 v3)	14
6.2.	PROTEÇÃO DA CHAVE PRIVADA	14
6.2.1.	Padrões para módulo criptográfico	14
6.2.2.	Controle "n de m" para chave privada	14
6.2.3.	Recuperação (escrow) de chave privada	14

6.2.4.Cópia de segurança (backup) de chave privada	14
6.2.5.Arquivamento de chave privada	14
6.2.6.Inserção de chave privada em módulo criptográfico	14
6.2.7.Método de ativação de chave privada	14
6.2.8.Método de desativação de chave privada	14
6.2.9.Método de destruição de chave privada	14
6.3.OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES	14
6.3.1.Arquivamento de chave pública.....	14
6.3.2.Períodos de uso para as chaves pública e privada.....	15
6.4.DADOS DE ATIVAÇÃO	15
6.4.1.Geração e instalação dos dados de ativação	15
6.4.2.Proteção dos dados de ativação	15
6.4.3.Outros aspectos dos dados de ativação.....	15
6.5.CONTROLES DE SEGURANÇA COMPUTACIONAL	15
6.5.1.Requisitos técnicos específicos de segurança computacional	15
6.5.2.Classificação da segurança computacional	15
6.6.CONTROLES TÉCNICOS DO CICLO DE VIDA	15
6.6.1.Controles de desenvolvimento de sistema	15
6.6.2.Controles de gerenciamento de segurança.....	15
6.6.3.Classificações de segurança de ciclo de vida.....	16
6.7.CONTROLES DE SEGURANÇA DE REDE	16
6.8.CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO	16
7. PERFIS DE CERTIFICADO E LCR.....	16
7.1.PERFIL DO CERTIFICADO	16
7.1.1.Número de versão.....	16
7.1.2.Extensões de certificado	16
7.1.3.Identificadores de algoritmo	19
7.1.4.Formatos de nome	19
7.1.5.Restrições de nome.....	21
7.1.6.OID (Object Identifier) de Política de Certificado.....	22
7.1.7.Uso da extensão “Policy Constraints”	22
7.1.8.Sintaxe e semântica dos qualificadores de política	22
7.1.9.Semântica de processamento para extensões críticas	22
7.2.PERFIL DE LCR	22
7.2.1.Número(s) de versão.....	22
7.2.2.Extensões de LCR e de suas entradas.....	22
8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO.....	22
8.1.PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO	22
8.2.POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO	22
8.3.PROCEDIMENTOS DE APROVAÇÃO	22
9. DOCUMENTOS REFERENCIADOS.....	23

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que a provou a alteração	Item Alterado	Descrição da Alteração
5.1	02/12/2015	Resolução 115, de 11.11.2015 (Versão 6.0)	1.1.3, 1.1.7, 1.3.5.7, 6.1.1.1.1, 6.2.4.1, 7.1.2.3 e 7.1.2.8	Referência aos parágrafos referentes à Política de Certificado A CF-e-SAT
5.2	29/11/2016	Resolução 116, de 09 de dezembro de 2015	6.1.5.1, 7.1.3, 7.1.2.2	Referencia à autoridade certificadora Raiz V5 e suas cadeias subsequentes
		Resolução 118, de 09 de dezembro de 2015	7.1.2.2, 7.2.2.2	Aprova a retirada do campo AIA da LCR e define a obrigatoriedade de dois pontos de obtenção da LCR em novas cadeias de certificação digital ICP-Brasil
		Instrução Normativa 07, de 15 de julho de 2016	7.1.2.2, 7.1.2.3, 9.2	Adequações exigidas pelo DOC- ICP-01.02: exclusão à referencia a certificados de equipamento e indicação de uso da AC para emissão de certificados de Assinatura Geral e Proteção de e-mail (S/MIME).

Política de Certificado de Assinatura Digital Tipo A3 da Autoridade Certificadora Certisign para a Justiça

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Esta “Política de Certificado” (PC) descreve as políticas de certificação de certificados de Assinatura Digital Tipo A3 da Autoridade Certificadora Certisign para a Justiça na Infraestrutura de Chaves Públicas Brasileira.

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

- 1.1.2. Não se aplica.
- 1.1.3. Não se aplica.
- 1.1.4. Não se aplica.
- 1.1.5. Não se aplica.
- 1.1.6. Não se aplica.
- 1.1.7. Não se aplica.
- 1.1.8. Não se aplica.

1.2. Identificação

1.2.1. Esta PC é chamada “Política de Certificado de assinatura digital Tipo A3 da Autoridade Certificadora Certisign para a Justiça” e referida como “PC A3 da AC Certisign-JUS”. Esta PC descreve os usos relacionados ao certificado de assinatura digital correspondente ao tipo A3 no DOC-ICP-04 do Comitê Gestor da ICP-Brasil. O OID (object identifier) desta PC é 2.16.76.1.2.3.21.

1.2.2. Não se aplica.

1.3. Comunidade e Aplicabilidade

1.3.1. Autoridades Certificadoras

1.3.1.1. Esta PC refere-se exclusivamente à AC Certisign-JUS no âmbito da ICP-Brasil.

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

1.3.2. Autoridades de Registro

1.3.2.1. Os dados a seguir, referentes às Autoridades de Registro – AR utilizadas pela AC Certisign-JUS para os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são publicados em serviço de diretório e/ou em página web da AC Certisign-JUS (<https://www.certisign.com.br/certisign/repositorios/icp-brasil/autoridades-registro/ac-certisign-jus>):

- 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 Certisign-JUS, 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 AR vinculadas com outras AR da ICP-Brasil, se for o caso.

1.3.2.2. A AC Certisign-JUS mantém as informações acima sempre atualizadas.

1.3.3. Prestador de Serviço de Suporte

1.3.3.1. A relação de todos os Prestadores de Serviço de Suporte – PSS vinculados diretamente a AC Certisign-JUS e/ou por intermédio de suas AR é publicada em serviço de diretório e/ou em página web da AC Certisign-JUS (<http://icp-brasil.certisign.com.br/repositorio/ac-certisign-jus/index.htm>).

1.3.3.2. PSS são entidades utilizadas pela AC e/ou suas AR para desempenhar atividade descrita na DPC ou nesta PC e se classificam em três categorias, conforme 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 Certisign-JUS mantém as informações acima sempre atualizadas.

1.3.4. Titulares de Certificado

Os certificados digitais Cert-JUS Institucional destinam-se exclusivamente aos agentes públicos do Poder Judiciário, autorizados pela autoridade competente do seu órgão de lotação a recebê-los e identificam os titulares do certificado não só como indivíduo, mas também como servidor do órgão do Poder Judiciário em que está lotado.

Os certificados digitais Cert-JUS Poder Público destinam-se exclusivamente a agentes públicos, autorizados pela autoridade competente do seu órgão de lotação, a recebê-los. O certificado Cert-JUS Poder Público identifica o titular do certificado não só como indivíduo, mas também como servidor do órgão público em que está lotado, sendo vedada a emissão do Cert-JUS Poder Público para servidores de órgãos do Poder Judiciário.

1.3.5. Aplicabilidade

1.3.5.1. Neste item são relacionadas as aplicações para as quais os certificados definidos por esta PC são adequados.

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

1.3.5.3. A AC Certisign-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 Cert-JUS Institucional e Cert-JUS Poder Público emitidos pela AC Certisign-JUS no âmbito desta PC serão utilizados, nos atos praticados pelos agentes públicos no exercício de suas funções, tais como assinatura de documentos e mensagens de correio eletrônico, criptografia, autenticação para acesso a sistemas e aplicações, login na rede e acesso remoto seguro. Por ser instrumento de identificação pessoal e institucional bem como de assinatura digital pessoal do titular, o uso do Cert-JUS Poder Público não é exclusivo para fins institucionais e profissionais, podendo ser utilizado para qualquer operação no meiodigital que utilize a tecnologia de certificação digital.

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

Nome:	Certisign Certificadora Digital S.A.
Endereço:	Rua Bela Cintra, 904 - 16. andar
Telefone:	(11) 4501-2417

Nome: Patricia T O Leite
Telefone: (11) 4501-2417
E-mail: icpbrasil@certisign.com.br

2. DISPOSIÇÕES GERAIS

Nos itens seguintes são referidos os itens correspondentes da DPC da AC Certisign-JUS.

- 2.1. Obrigações e Direitos**
 - 2.1.1. Obrigações da AC Certisign-JUS**
 - 2.1.2. Obrigações das AR**
 - 2.1.3. Obrigações do Titular do Certificado**
 - 2.1.4. Direitos da Terceira Parte (Relying Party)**
 - 2.1.5. Obrigações do Repositório**
- 2.2. Responsabilidades**
 - 2.2.1. Responsabilidades da AC Certisign-JUS**
 - 2.2.2. Responsabilidades das AR**
- 2.3. Responsabilidade Financeira**
 - 2.3.1. Indenizações devidas pela terceira parte(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 da solução de disputa**
- 2.5. Tarifas de Serviço**
 - 2.5.1. Tarifas de emissão e renovação de certificados**
 - 2.5.2. Tarifas de acesso ao certificado**
 - 2.5.3. Tarifas de revogação ou de acesso à informação de status**
 - 2.5.4. Tarifas para outros serviços**
 - 2.5.5. Política de reembolso**
- 2.6. Publicação e Repositório**
 - 2.6.1. Publicação de informação da AC Certisign-JUS**
 - 2.6.2. Frequência de publicação**
 - 2.6.3. Controles de acesso**
 - 2.6.4. Repositórios**
- 2.7. Fiscalização e Auditoria de Conformidade**
- 2.8. Sigilo**
 - 2.8.1. Disposições gerais**
 - 2.8.2. Tipos de informações sigilosas**
 - 2.8.3. Tipos de informações não sigilosas**
 - 2.8.4. Divulgação de informação de revogação ou suspensão de certificado**
 - 2.8.5. Quebra de sigilo por motivos legais**
 - 2.8.6. Informações a terceiros**
 - 2.8.7. Divulgação por solicitação do Titular**
 - 2.8.8. Outras circunstâncias de divulgação de informação**
- 2.9. Direitos de Propriedade Intelectual**

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

Nos itens seguintes são referidos os itens correspondentes da DPC da AC Certisign-JUS.

3.1. Registro Inicial

- 3.1.1. Disposições Gerais**
- 3.1.2. Tipos de nomes**
- 3.1.3. Necessidade de nomes significativos**
- 3.1.4. Regras para interpretação de vários tipos de nomes**
- 3.1.5. Unicidade de nomes**
- 3.1.6. Procedimento para resolver disputa de nomes**
- 3.1.7. Reconhecimento, autenticação e papel de marcas registradas**
- 3.1.8. Método para comprovar a posse de chave privada**
- 3.1.9. Autenticação da identidade de um indivíduo**
 - 3.1.9.1. Documentos para efeitos de identificação de um indivíduo**
 - 3.1.9.2. Informações contidas no certificado emitido para um indivíduo**
- 3.1.10. Autenticação da identidade de uma organização**
 - 3.1.10.1. Disposições Gerais**
 - 3.1.10.2. Documentos para efeitos de identificação de uma organização**
 - 3.1.10.3. Informações contidas no certificado emitido para uma organização**
- 3.1.11. Autenticação da identidade de equipamento ou aplicação**
 - 3.1.11.1. Disposições Gerais**
 - 3.1.11.2. Procedimentos para efeitos de identificação de um equipamento ou aplicação**
 - 3.1.11.3. Informações contidas no certificado emitido para um equipamento ou aplicação**
- 3.1.12. Autenticação de identificação de equipamento para certificado CF-e-SAT**
- 3.2. Geração de novo par de chaves antes da expiração do atual**
- 3.3. Geração de novo par de chaves após expiração ou revogação**
- 3.4. Solicitação de Revogação**

4. REQUISITOS OPERACIONAIS

Nos itens seguintes são referidos os itens correspondentes da DPC da AC Certisign-JUS.

- 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 ou 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 eventos 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 arquivo
 - 4.6.4. Procedimentos para cópia de segurança (backup) de arquivo
 - 4.6.5. Requisitos para datação (time-stamping) de registros
 - 4.6.6. Sistema de coleta de dados de arquivo
 - 4.6.7. Procedimentos para obter e verificar informação de arquivo
- 4.7. Troca de chave
- 4.8. Comprometimento e Recuperação de Desastre
 - 4.8.1. Recursos computacionais, *software*, e dados corrompidos
 - 4.8.2. Certificado de entidade é revogado
 - 4.8.3. Chave da entidade é comprometida
 - 4.8.4. Segurança dos recursos após desastre natural ou de outra natureza
 - 4.8.5. Atividades das Autoridades de Registro
- 4.9. Extinção dos serviços de AC, AR ou PSS

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Nos itens seguintes são referidos os itens correspondentes da DPC da AC Certisign-JUS.

- 5.1. Controles Físicos
 - 5.1.1. Construção e localização das instalações
 - 5.1.2. Acesso físico nas instalações de AC
 - 5.1.2.1. Níveis de acesso
 - 5.1.2.2. Sistemas físicos de detecção
 - 5.1.2.3. Sistema de controle de acesso
 - 5.1.2.4. Mecanismos de emergência
 - 5.1.3. Energia e ar condicionado nas instalações de AC
 - 5.1.4. Exposição à água nas instalações de AC
 - 5.1.5. Prevenção e proteção contra incêndio nas instalações de AC
 - 5.1.6. Armazenamento de mídia nas instalações de AC

- 5.1.7. **Destruição de lixo nas instalações de AC**
- 5.1.8. **Instalações de segurança (backup) externas (off-site) para AC**
- 5.1.9. **Instalações técnicas de AR**
- 5.2. **Controles Procedimentais**
 - 5.2.1. **Perfis qualificados**
 - 5.2.2. **Número de pessoas necessário por tarefa**
 - 5.2.3. **Identificação e autenticação para cada perfil**
- 5.3. **Controles de Pessoal**
 - 5.3.1. **Antecedentes, qualificação, experiência e requisitos de idoneidade**
 - 5.3.2. **Procedimentos de verificação de antecedentes**
 - 5.3.3. **Requisitos de treinamento**
 - 5.3.4. **Frequência e requisitos para reciclagem técnica**
 - 5.3.5. **Frequência e sequencia de rodízio de cargos**
 - 5.3.6. **Sanções para ações não autorizadas**
 - 5.3.7. **Requisitos para contratação de pessoal**
 - 5.3.8. **Documentação fornecida ao pessoal**

6. CONTROLES TÉCNICOS DE SEGURANÇA

6.1. Geração e Instalação do Par de Chaves

6.1.1. Geração do par de chaves

6.1.1.1. O par de chaves criptográficas é gerado pelo titular do certificado, quando este for uma pessoa física. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(is), a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.

6.1.1.1.1. Não se aplica.

6.1.1.2. A geração do par de chaves criptográficas ocorre, no mínimo, utilizando CSP (Cryptographic Service Provider) existente na estação do solicitante apresentados pelo browser.

A geração do par de chaves criptográficas ocorre utilizando cartão inteligente ou token ambos com capacidade de geração de chave protegidos por senha.

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

6.1.1.4. Ao ser gerada, a chave privada do titular do certificado deve ser gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1]. As chaves privadas correspondentes aos certificados deverão ser armazenadas em cartão inteligente ou token, ambos com capacidade de geração de chave, sendo ativados e protegidos por senha e/ou identificação biométrica.

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

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

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

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

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

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

O tipo de certificado emitido pela AC Certisign-JUS é descrito nesta PC é o A3.

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
A3	Cartão Inteligente ou Token, ambos com capacidade de geração de chave e protegidos por senha e/ou identificação biométrica, ou hardware criptográfico homologado junto à ICP-Brasil.

6.1.1.8. A responsabilidade pela adoção de controles de segurança para a garantia do sigilo, integridade e disponibilidade da chave privada gerada no equipamento é do titular do certificado, conforme especificado no Termo de Titularidade, no caso de certificados de pessoa física, e da pessoa responsável, indicada por seus(s) representante(s) legal(s), conforme especificado no Termo de Responsabilidade, no caso de certificados de pessoa jurídica e aplicações.

6.1.2. Entrega da chave privada à entidade titular do certificado

Não se aplica.

6.1.3. Entrega da chave pública para emissor de certificado

A entrega da chave pública do solicitante do certificado, é feita por meio eletrônico, em formato PKCS#10, através de uma sessão segura SSL - Secure Socket Layer.

6.1.4. Disponibilização de chave pública da AC para usuários

A AC Certisign-JUS disponibiliza o seu certificado, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, através de endereço Web: http://icp-brasil.certisign.com.br/repositorio/certificados/AC_Certisign_JUS_G3.p7c (para cadeia V2) e http://icp-brasil.certisign.com.br/repositorio/certificados/AC_Certisign_JUS_G6.p7c (para cadeia V5).

6.1.5. Tamanhos de chave

6.1.5.1. O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC Certisign-JUS é de 1024 bits para a hierarquia V1 e de 2048 bits para a hierarquia V2 e V5.

6.1.5.2. Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo A3 da ICP-Brasil está definido 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 certificados adotam, no mínimo, o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.7. Verificação da qualidade dos parâmetros

Os parâmetros são 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

A geração das chaves criptográficas do Certificado Tipo A3 desta PC, é realizada 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)

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

Os pares de chaves correspondentes aos certificados emitidos pela AC Certisign-JUS podem ser utilizados para a assinatura digital (chave privada), para a verificação dela (chave pública), para a garantia do não repúdio e para cifragem de chaves.

6.2. Proteção da Chave Privada

6.2.1. Padrões para módulo criptográfico

Não se aplica.

6.2.2. Controle “n de m” para chave privada

Não se aplica.

6.2.3. Recuperação (escrow) de chave privada

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

6.2.4. Cópia de segurança (backup) de chave privada

6.2.4.1. Não é permitido backup para certificados emitidos por esta PC.

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

6.2.4.3. Não se aplica.

6.2.4.4. Não se aplica.

6.2.5. Arquivamento de chave privada

6.2.5.1. A AC Certisign-JUS não arquiva cópias de chaves privadas de assinatura digital de titulares de certificados.

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

6.2.6. Inserção de chave privada em módulo criptográfico

Não se aplica.

6.2.7. Método de ativação de chave privada

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

6.2.8. Método de desativação de chave privada

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

6.2.9. Método de destruição de chave privada

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

6.3. Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1. Arquivamento de chave pública

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

6.3.2.Períodos de uso para as chaves pública e privada

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

6.3.2.2. Não se aplica.

6.3.2.3. O período máximo de validade admitido para certificados de assinatura digital Tipo A3 da AC Certisign-JUS é de 3 (três) anos.

6.4.Dados de Ativação

6.4.1.Geração e instalação dos dados de ativação

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

6.4.2.Proteção dos dados de ativação

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

6.4.3.Outros aspectos dos dados de ativação

Não se aplica.

6.5.Controles de Segurança Computacional

6.5.1.Requisitos técnicos específicos de segurança computacional

O titular do certificado é responsável pela segurança computacional dos sistemas nos quais são geradas e utilizadas as chaves privadas e deve zelar por sua integridade.

O equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados possui conexão com o dispositivo de mídia inteligente e o respectivo driver instalado. A mídia inteligente possui processador criptográfico com capacidade de geração interna das chaves.

6.5.2.Classificação da segurança computacional

Não se aplica.

6.6.Controles Técnicos do Ciclo de Vida

A AC Certisign-JUS desenvolve sistemas apenas com finalidade relacionada à operação de suas AR vinculadas.

6.6.1.Controles de desenvolvimento de sistema

6.6.1.1. A AC Certisign-JUS utiliza os modelos clássico espiral e SCRUM no desenvolvimento dos sistemas, de acordo com a melhor adequação destes modelos ao projeto em desenvolvimento. São realizadas as fases de requisitos, análise, projeto, codificação e teste para cada interação do sistema utilizando tecnologias de orientação a objetos. Como suporte a esse modelo, a AC Certisign-JUS utiliza uma gerência de configuração, gerência de mudança, testes formais e outros processos.

6.6.1.2. Os processos de projeto e desenvolvimento conduzidos pela AC Certisign-JUS provêm documentação suficiente para suportar avaliações externas de segurança dos componentes da AC Certisign-JUS.

6.6.2.Controles de gerenciamento de segurança

6.6.2.1. A AC Certisign-JUS verifica os níveis configurados de segurança com periodicidade semanal e através de ferramentas do próprio sistema operacional. As verificações são feitas através da emissão de comandos de sistema e comparando-se com as configurações

aprovadas. Em caso de divergência, são tomadas as medidas para recuperação da situação, conforme a natureza do problema e averiguação do fato gerador do problema para evitar sua recorrência.

6.6.2.2. A AC Certisign-JUS utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

6.6.3. Classificações de segurança de ciclo de vida

Não se aplica.

6.7. Controles de Segurança de Rede

Não se aplica.

6.8. Controles de Engenharia do Módulo Criptográfico

Não se aplica.

7. PERFIS DE CERTIFICADO E LCR

7.1. Perfil do Certificado

Todos os certificados emitidos pela AC Certisign-JUS estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.1.1. Número de versão

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

7.1.2. Extensões de certificado

7.1.2.1. Neste item, a PC descreve todas as extensões de certificado utilizadas pela AC Certisign-JUS e sua criticalidade.

7.1.2.2. Extensões Obrigatórias:

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

- a) **Authority Key Identifier**, não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da AC Certisign-JUS;
- b) **Key Usage**, crítica: somente os bits digitalSignature, nonRepudiation e keyEncipherment estão ativados;
- c) **Certificate Policies**, não crítica contém:
 - O OID desta PC: 2.16.76.1.2.3.21;
 - Os campos policyQualifiers contém o endereço Web da DPC AC Certisign-JUS:
http://icp-brasil.certisign.com.br/repositorio/dpc/AC_Certisign_JUS/DPC_AC_Certisign_JUS.pdf;

- d) **CRL Distribution Points**, não crítica: contém os endereços Web onde se obtém a LCR da AC Certisign-JUS:

Para certificados emitidos na G2:

<http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisign-JUSG2/LatestCRL.crl>
<http://icp-brasil.outralcr.com.br/repositorio/lcr/ACCertisign-JUSG2/LatestCRL.crl>
<http://repositorio.icpbrasil.gov.br/lcr/Certisign/ACCertisign-JUSG2/LatestCRL.crl>

Para certificados emitidos na G3:

<http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisign-JUSG3/LatestCRL.crl>
<http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisign-JUSG3/LatestCRL.crl>
<http://repositorio.icpbrasil.gov.br/lcr/Certisign/ACCertisign-JUSG3/LatestCRL.crl>

Para certificados emitidos na V5:

<http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisign-JUSG6/LatestCRL.crl>
<http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisign-JUSG6/LatestCRL.crl>

e) **Authority Information Access**, não crítica: contém o endereço de acesso aos certificados da cadeia de certificação através do link:

Para certificados emitidos na G3:

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_Certisign_JUS_G3.p7c

Para certificados emitidos na V5:

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_Certisign_JUS_G6.p7c;

e o endereço de acesso ao serviço de Consulta On-Line de Situação de Certificado (On-line Certificate Status Protocol- OCSP):

Para certificados emitidos na G3: <http://ocsp.certisign.com.br>

Para certificados emitidos na V5: <http://ocsp-ac-certisign-jus.certisign.com.br>

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

7.1.2.3. Os certificados emitidos pela AC Certisign-JUS possuem a extensão "Subject Alternative Name", não crítica e com os seguintes formatos:

a) Para certificado Cert-JUS Institucional e Poder Público:

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

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

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

iii. 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.

iv. rfc822Name contendo o e-mail institucional do titular do certificado. Este campo deverá estar no formato IA5string

a.2) campo otherName, não obrigatório, contendo:

i. OID = 1.3.6.1.4.1.311.20.2.3 e conteúdo = Nome Principal que contém o domínio de login em estações de trabalho (UPN).

b) não se aplica

c) Para certificado de aplicação:

c.1) 5 (cinco) campos otherName, obrigatórios, contendo, nesta ordem:

- i. OID = 2.16.76.1.3.8 e conteúdo = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, se o certificado for de pessoa jurídica;
- ii. OID = 2.16.76.1.3.3 e conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ), se o certificado for de pessoa jurídica;
- iii. OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado;
- iv. OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições 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;
- v. rfc822Name, contendo o e-mail institucional do responsável pelo certificado. Este campo deverá estar no formato IA5string.

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

- a) não se aplica;
- b) não se aplica;
- c) O conjunto de informações definido em cada campo otherName é armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING ou PRINTABLE STRING, com exceção do campo UPN que possui uma cadeia de caracteres do tipo ASN.1 UTF8 STRING;
- d) Quando os números de NIS (PIS, PASEP ou CI), RG, CEI ou Título de Eleitor não estiverem disponíveis, os campos correspondentes são integralmente preenchidos com caracteres "zero";
- e) Se o número do RG não estiver disponível, não é preenchido o campo de órgão emissor/UF. O mesmo ocorre para o campo do município e UF se não houver número de inscrição do Título de Eleitor;
- f) Todas as informações de tamanho variável, referentes a números, tal como RG, são preenchidos com caracteres "zero" a sua esquerda para que seja completado seu máximo tamanho possível;
- g) As 10 (dez) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, sendo utilizados apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF do Título de Eleitor;

h) Apenas os caracteres de A a Z, de 0 a 9, observado o disposto no item 7.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais, com exceção do campo UPN que utiliza caracteres especiais;

i) não se aplica;

j) não se aplica;

k) O campo UPN é opcional, caso não seja usado o OID não é incluído no certificado.

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

Campos otherName não obrigatórios quando não utilizados não terão seus OID incluído no certificado.

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

7.1.2.7. Não se aplica.

7.1.2.8 Não se aplica.

7.1.2.9. A AC Certisign-JUS implementa a extensão "Extended Key Usage", não crítica:

a) Para certificados de assinatura de resposta OCSP: somente o propósito "OCSP Signing" (OID 1.3.6.1.5.5.7.3.9) está ativado;

b) Para os demais certificados de Assinatura e/ou Proteção de e-mail:

(i) os propósitos "client authentication" (OID 1.3.6.1.5.5.7.3.2) e "E-mail protection" (OID 1.3.6.1.5.5.7.3.4) estão ativados;

(ii) o propósito "Smart Card Logon" (OID 1.3.6.1.4.1.311.20.2.2) pode estar ativado, quando for utilizado o campo "UPN" na extensão "Subject Alternative Name".

7.1.3. Identificadores de algoritmo

Os certificados emitidos pela AC Certisign-JUS são assinados com o uso do algoritmo RSA com SHA-1 como função de hash (OID 1.2.840.113549.1.1.5) na hierarquia V1, algoritmo RSA com SHA-256 como função de hash (OID 1.2.840.113549.1.1.11) ou algoritmo RSA com SHA-512 como função de hash (OID 1.2.840.113549.1.1.13) nas hierarquias V2 e V5 conforme o padrão PKCS#1.

7.1.4. Formatos de nome

O nome do titular do certificado, constante do campo "Subject", adota o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

De forma geral:

- i. Nos formatos abaixo, os caracteres "<" e ">" delimitam campos que serão substituídos pelos seus respectivos valores; os caracteres "<" e ">" não devem ser incluídos.
- ii. Os dados necessários para preenchimento do DN deverão ser os informados na AUTORIZAÇÃO citada no item 3.1.9.1 ou 3.1.10.2 da DPC.
- iii. Todos os campos do DN são obrigatórios e devem ser preenchidos.
- iv. O tamanho máximo de cada componente do DN (C,CN,O,OU,etc) é de 64 caracteres.

Cert-JUS Institucional

- I. O conteúdo do DN apresenta-se da seguinte forma para os certificados Cert-JUS Institucional:

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> : <#####>

No CN, caso o nome completo do titular exceda os 54 caracteres, deverá ser escrito até o limite de 54 caracteres, vedada a abreviatura.

Os caracteres “#” representam os dígitos da matrícula do titular. Todos os outros caracteres devem ser interpretados literalmente.

Os últimos nove caracteres do campo CN (Common Name) devem ser o nº de matrícula do titular no órgão de lotação, completado com caracteres brancos à direita, caso possua tamanho menor do que 9 caracteres.

A AUTORIZAÇÃO citada no item 3.1.9.1 da DPC deverá conter também o UPN(nome de login do Window) na forma *usuário@domínio_institucional*, se for de interesse da instituição.

Para o certificado Cert-JUS Institucional, exclusivo para o Poder Judiciário, a informação <Cargo do Titular> deverá ser preenchido SOMENTE com uma das seguintes opções:

- MAGISTRADO;
- SERVIDOR;
- PRESTADOR DE SERVIÇO; ou
- ESTAGIÁRIO.

- II. órgãos autorizados:

A lista de órgãos cadastrados, bem como as respectivas siglas padronizadas, está publicada no repositório da AC-JUS (<http://www.acjus.jus.br/repositorio/Outros>) e é divulgada para todas as Autoridades Certificadoras da cadeia AC-JUS.

Em caso de dúvida sobre a padronização de nomes ou siglas de órgãos não constantes da lista publicada a unidade administrativa da AC-JUS deve ser consultada.

Cert-JUS Poder Público

- I. O conteúdo do DN apresenta-se da seguinte forma para os certificados Cert-JUS Poder Público:

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 do órgão>
OU = <Cargo do Titular>
CN = <Nome do Titular> : <#####>

No CN, caso o nome completo do titular exceda os 54 caracteres, deverá ser escrito até o limite de 54 caracteres, vedada a abreviatura.

Os caracteres “#” representam os dígitos da matrícula do titular. Todos os outros caracteres devem ser interpretados literalmente.

Os últimos nove caracteres do campo CN (Common Name) devem ser o nº de matrícula do titular no órgão de lotação, completado com caracteres brancos à direita, caso possua tamanho menor do que 9 caracteres.

A AUTORIZAÇÃO citada no item 3.1.9.1 da DPC deverá conter também o UPN (nome de login do Window) na forma *usuário@domínio_institucional*, se for de interesse da instituição.

II. órgãos autorizados:

Órgãos não pertencentes ao Poder Judiciário deverão solicitar CADASTRAMENTO junto à AC-JUS, para a emissão de certificados Cert-JUS, sendo que a AC Certisign-JUS somente emitirá o certificados digitais para órgãos não pertencentes ao Poder Judiciário após o CADASTRAMENTO ter sido aprovado pela AC-JUS.

O cadastramento deve ser solicitado por ofício da autoridade competente do órgão interessado, endereçado à AC-JUS.

Após a aprovação do cadastro a AC-JUS oficiará as AC subsequentes para que incluam o órgão cadastrado nos seus sistemas de certificação. O nome e sigla do órgão deverão ser aquelas constantes da comunicação de cadastramento encaminhada pela AC-JUS à AC emitente.

A lista de órgãos cadastrados, bem como as respectivas siglas padronizadas, está publicada no repositório da AC-JUS (<http://www.acjus.jus.br/repositorio/Outros>) e é divulgada para todas as Autoridades Certificadoras da cadeia AC-JUS.

Em caso de dúvida sobre a padronização de nomes ou siglas de órgãos não constantes da lista publicada a unidade administrativa da AC-JUS deve ser consultada.

7.1.5. Restrições de nome

7.1.5.1. Neste item da PC, devem ser descritas as restrições aplicáveis para os nomes dos titulares de certificados.

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

- Não são admitidos sinais de acentuação, trema ou cedilhas;
- Apenas são admitidos sinais alfanuméricos e os caracteres especiais descritos na tabela abaixo:

Caractere	Código NBR9611 (hexadecimal)
Branco	20
"	22
#	23
'	27
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D

7.1.6.OID (Object Identifier) de Política de Certificado

O OID desta PC é 2.16.76.1.2.3.21.

Todo certificado emitido segundo essa PC, PC A3 AC Certisign-JUS, contém o valor desse OID presente na extensão Certificate Policies.

7.1.7.Uso da extensão “Policy Constraints”

Não se aplica.

7.1.8.Sintaxe e semântica dos qualificadores de política

Os campos policyQualifiers da extensão “Certificate Policies” contém o endereço web da DPC da AC Certisign-JUS (http://icp-brasil.certisign.com.br/repositorio/dpc/AC_Certisign_JUS/DPC_AC_Certisign_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(s) de versão

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

7.2.2.Extensões de LCR e de suas entradas

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

7.2.2.2. As LCR da AC Certisign-JUS obedecem a ICP - Brasil que define como obrigatórias as seguintes extensões:

- a) **Authority Key Identifier**, não crítica: contém o hash SHA-1 da chave pública da AC Certisign-JUS;
- b) **CRL Number**, não crítica: contém um número sequencial para cada LCR emitida pela AC Certisign-JUS.

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1.Procedimentos de mudança de especificação

Alterações nesta PC podem ser solicitadas e/ou definidas pelo Grupo de Práticas e Políticas da AC Certisign-JUS. A aprovação e consequente adoção de nova versão estarão sujeitas à autorização da AC Raiz.

8.2.Políticas de publicação e notificação

A AC Certisign-JUS mantém página específica com a versão corrente desta PC para consulta pública, a qual está disponibilizada no endereço Web http://icp-brasil.certisign.com.br/repositorio/pc/AC_Certisign_JUS/PC_A3_AC_Certisign_JUS_v5.2.pdf.

8.3.Procedimentos de aprovação

Esta PC da AC Certisign-JUS foi submetida à aprovação, durante o processo de credenciamento da AC Certisign-JUS, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

Novas versões serão igualmente submetidas à aprovação da AC Raiz.

9. DOCUMENTOS REFERENCIADOS

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

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

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

Ref.	Nome do documento	Código
[1]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01
[2]	ATRIBUIÇÃO DE OID NA ICP-BRASIL	DOC-ICP-04.01
[4]	REQUISITOS ADICIONAIS PARA ADERÊNCIA AOS PROGRAMAS DE RAÍZES CONFIÁVEIS	DOC-ICP-01.02