

**Política de Certificado de Assinatura
Digital Tipo A1
da Autoridade Certificadora Certisign
Múltipla**

PC A1 DA AC Certisign Múltipla

Versão 3.2 – 08 de Dezembro de 2011

ÍNDICE

1. INTRODUÇÃO	6
1.1. VISÃO GERAL.....	6
1.2. IDENTIFICAÇÃO.....	6
1.3. COMUNIDADE E APLICABILIDADE.....	6
1.3.1. Autoridades Certificadoras	6
1.3.2. Autoridades de Registro	7
1.3.3. Prestador de Serviço de Suporte.....	7
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.....	10
2.1.1. Obrigações da AC Certisign Múltipla.....	10
2.1.2. Obrigações das AR.....	10
2.1.3. Obrigações dos Titulares do Certificado.....	10
2.1.4. Direitos da Terceira Parte (Relying Party).....	10
2.1.5. Obrigações do Repositório.....	10
2.2. RESPONSABILIDADES.....	10
2.2.1. Responsabilidades da AC Certisign Múltipla	10
2.2.2. Responsabilidades das AR	10
2.3. RESPONSABILIDADE FINANCEIRA.....	10
2.3.1. Indenizações devidas pela terceira parte (Relying Party).....	10
2.3.2. Relações Fiduciárias.....	10
2.3.3. Processos Administrativos	10
2.4. INTERPRETAÇÃO E EXECUÇÃO	10
2.4.1. Legislação	10
2.4.2. Forma de interpretação e notificação.....	10
2.4.3. Procedimentos de solução de disputa.....	10
2.5. TARIFAS DE SERVIÇO.....	10
2.5.1 Tarifas de emissão e renovação de certificados.....	10
2.5.2 Tarifas de acesso ao certificado	10
2.5.3 Tarifas de revogação ou de acesso à informação de status.....	10
2.5.4 Tarifas para outros serviços.....	10
2.5.5 Política de reembolso.....	10
2.6. PUBLICAÇÃO E REPOSITÓRIO	10
2.6.1 Publicação de informação da AC.....	10
2.6.2. Freqüência de publicação.....	11
2.6.3. Controles de acesso	11
2.6.4. Repositórios.....	11
2.7. AUDITORIA E FISCALIZAÇÃO	11
2.8. SIGILO.....	11
2.8.1. Tipos de informações sigilosas	11
2.8.2. Tipos de informações não-sigilosas	11
2.8.3. Divulgação de informação de revogação ou suspensão de certificado	11
2.8.4. Quebra de sigilo por motivos legais.....	11
2.8.5. Informações a terceiros.....	11
2.8.6. Divulgação por solicitação do Titular do Certificado.....	11
2.8.7. Outras circunstâncias de divulgação de informação	11
2.9. DIREITOS DE PROPRIEDADE INTELECTUAL.....	11

3. IDENTIFICAÇÃO E AUTENTICAÇÃO	11
3.1. REGISTRO INICIAL	12
3.1.1. Disposições Gerais.....	12
3.1.2. Tipos de nomes.....	12
3.1.3. Necessidade de nomes significativos	12
3.1.4. Regras para interpretação de vários tipos de nomes	12
3.1.5. Unicidade de nomes.....	12
3.1.6. Procedimento para resolver disputa de nomes.....	12
3.1.7. Reconhecimento, autenticação e papel de marcas registradas	12
3.1.8. Método para comprovar a posse de chave privada	12
3.1.9. Autenticação da identidade de uma organização	12
3.1.9. Autenticação da identidade do indivíduo	12
3.1.9.1. Documentos para efeitos de identificação de um indivíduo	12
3.1.9.2. Informações contidas no certificado emitido para um indivíduo	12
3.1.10. Autenticação da identidade de uma organização.....	12
3.1.10.1. Disposições Gerais.....	12
3.1.10.2. Documentos para efeitos de identificação de uma organização	12
3.1.10.3. Informações contidas no certificado emitido para uma organização	12
3.1.11. Autenticação da identidade de um equipamento ou aplicação.....	12
3.1.10.1. Disposições Gerais.....	12
3.1.10.2. Procedimentos para efeitos de identificação de um equipamento ou aplicação	12
3.1.10.3. Informações contidas no certificado emitido para um equipamento ou aplicação	12
3.2. GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL	12
3.3. GERAÇÃO DE NOVO PAR DE CHAVES APÓS REVOGAÇÃO.....	12
3.4. SOLICITAÇÃO DE REVOGAÇÃO	13
4. REQUISITOS OPERACIONAIS	13
4.1. SOLICITAÇÃO DE CERTIFICADO.....	13
4.2. EMISSÃO DE CERTIFICADO	13
4.3. ACEITAÇÃO DE CERTIFICADO	13
4.4. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO	13
4.4.1. Circunstâncias para revogação.....	13
4.4.2. Quem pode solicitar revogação	13
4.4.3. Procedimento para solicitação de revogação	14
4.4.4. Prazo para solicitação de revogação	14
4.4.5. Circunstâncias para suspensão.....	14
4.4.6. Quem pode solicitar suspensão.....	14
4.4.7. Procedimento para solicitação de suspensão.....	14
4.4.8. Limites no período de suspensão.....	14
4.4.9. Frequência de emissão de LCR.....	14
4.4.10. Requisitos para verificação de LCR.....	14
4.4.11. Disponibilidade para revogação ou verificação de status on-line	14
4.4.12. Requisitos para verificação de revogação on-line.....	14
4.4.13. Outras formas disponíveis para divulgação de revogação	14
4.4.14. Requisitos para verificação de outras formas de divulgação de revogação	14
4.4.15. Requisitos especiais para o caso de comprometimento de chave.....	14
4.5. PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA	14
4.5.1. Tipos de eventos registrados.....	14
4.5.2. Frequência de auditoria de registros (logs).....	14
4.5.3. Período de retenção para registros (logs) de auditoria.....	14
4.5.4. Proteção de registro (log) de auditoria	14
4.5.5. Procedimentos para cópia de segurança (backup) de registro (log) de auditoria	14
4.5.6. Sistema de coleta de dados de auditoria.....	14

4.5.7. Notificação de agentes causadores de eventos.....	14
4.5.8. Avaliações de vulnerabilidade.....	14
4.6. ARQUIVAMENTO DE REGISTROS.....	14
4.6.1. Tipos de registros arquivados.....	14
4.6.2. Período de retenção para arquivo.....	15
4.6.3. Proteção de arquivo.....	15
4.6.4. Procedimentos para cópia de segurança (backup) de arquivo.....	15
4.6.5. Requisitos para datação (time-stamping) de registros.....	15
4.6.6. Sistema de coleta de dados de arquivo.....	15
4.6.7. Procedimentos para obter e verificar informação de arquivo.....	15
4.7. TROCA DE CHAVE.....	15
4.8. COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE.....	15
4.8.1. Recursos computacionais, software, e dados corrompidos.....	15
4.8.2. Certificado de entidade é revogado.....	15
4.8.3. Chave de entidade é comprometida.....	15
4.8.4. Segurança dos recursos após desastre natural ou de outra natureza.....	15
4.8.5. Atividades das Autoridades de Registro.....	15
4.9. EXTINÇÃO DOS SERVIÇOS DE AC, AR OU PSS.....	15
5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL.....	15
5.1. CONTROLES FÍSICOS.....	16
5.1.1. Construção e localização das instalações.....	16
5.1.2. Acesso físico.....	16
5.1.3. Energia e ar condicionado.....	16
5.1.4. Exposição à água.....	16
5.1.5. Prevenção e proteção contra incêndio.....	16
5.1.6. Armazenamento de mídia.....	16
5.1.7. Destruição de lixo.....	16
5.1.8. Instalações de segurança (backup) externas (off-site).....	16
5.2. CONTROLES PROCEDIMENTAIS.....	16
5.2.1. Perfis qualificados.....	16
5.2.2. Número de pessoas necessário por tarefa.....	16
5.2.3. Identificação e autenticação para cada perfil.....	16
5.3. CONTROLES DE PESSOAL.....	16
5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade.....	16
5.3.2. Procedimentos de verificação de antecedentes.....	16
5.3.3. Requisitos de treinamento.....	16
5.3.4. Frequência e requisitos para reciclagem técnica.....	16
5.3.5. Frequência e seqüência de rodízio de cargos.....	16
5.3.6. Sanções para ações não autorizadas.....	16
5.3.7. Requisitos para contratação de pessoal.....	16
5.3.8. Documentação fornecida ao pessoal.....	16
6. CONTROLES TÉCNICOS DE SEGURANÇA.....	16
6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES.....	16
6.1.1. Geração do par de chaves.....	17
6.1.2. Entrega da chave privada à entidade titular do certificado.....	18
6.1.3. Entrega da chave pública para emissor de certificado.....	18
6.1.4. Disponibilização de chave pública da AC para usuários.....	18
6.1.5. Tamanhos de chave.....	18
6.1.6. Geração de parâmetros de chaves assimétricas.....	18
6.1.7. Verificação da qualidade dos parâmetros.....	19
6.1.8. Geração de chave por hardware ou software.....	19
6.1.9. Propósitos de uso de chave (conforme o campo "key usage" na X.509 v3).....	19

6.2. PROTEÇÃO DA CHAVE PRIVADA	19
6.2.1. Padrões para módulo criptográfico	19
6.2.2. Controle "n de m" para chave privada	19
6.2.3. Recuperação (escrow) de chave privada	19
6.2.4. Cópia de segurança (backup) de chave privada	19
6.2.5. Arquivamento de chave privada	20
6.2.6. Inserção de chave privada em módulo criptográfico	20
6.2.7. Método de ativação de chave privada	20
6.2.8. Método de desativação de chave privada	20
6.2.9. Método de destruição de chave privada	20
6.3. OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES	20
6.3.1. Arquivamento de chave pública	20
6.3.2. Períodos de uso para as chaves pública e privada	21
6.4. DADOS DE ATIVAÇÃO	21
6.4.1. Geração e instalação dos dados de ativação	21
6.4.2. Proteção dos dados de ativação	21
6.4.3. Outros aspectos dos dados de ativação	21
6.5. CONTROLES DE SEGURANÇA COMPUTACIONAL	21
6.5.1. Requisitos técnicos específicos de segurança computacional	21
6.5.2. Classificação da segurança computacional	21
6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA	22
6.6.1. Controles de desenvolvimento de sistema	22
6.6.2. Controles de gerenciamento de segurança	22
6.6.3. Classificações de segurança de ciclo de vida	22
6.7. CONTROLES DE SEGURANÇA DE REDE	22
6.8. CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO	22
7. PERFIS DE CERTIFICADO E LCR	23
7.1. PERFIL DO CERTIFICADO	23
7.1.1. Número de versão	23
7.1.2. Extensões de certificado	23
7.1.3. Identificadores de algoritmo	27
7.1.4. Formatos de nome	28
7.1.5. Restrições de nome	28
7.1.6. OID (Object Identifier) de Política de Certificado	29
7.1.7. Uso da extensão "Policy Constraints"	29
7.1.8. Sintaxe e semântica dos qualificadores de política	29
7.1.9. Semântica de processamento para extensões críticas	29
7.2. PERFIL DE LCR	29
7.2.1. Número(s) de versão	29
7.2.2. Extensões de LCR e de suas entradas	<i>Erro! Indicador não definido.</i>
8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO	30
8.1. PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO	30
8.2. POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO	30
8.3. PROCEDIMENTOS DE APROVAÇÃO	30
9. DOCUMENTOS REFERENCIADOS	30

Política de Certificado de Assinatura Digital Tipo A1 da Autoridade Certificadora CERTISIGN MÚLTIPLA

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 A1 da Autoridade Certificadora Certisign Múltipla na Infra-estrutura 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 2527 (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.

1.2. Identificação

1.2.1. Esta PC é chamada “Política de Certificado de Assinatura Digital Tipo A1 da Autoridade Certificadora Certisign Múltipla” e referida como “PC A1 da AC Certisign Múltipla”. Esta PC descreve os usos relacionados ao certificado de Assinatura Digital correspondente ao tipo A1 do DOC-ICP-04 do Comitê Gestor da ICP-Brasil. O OID (object identifier) desta PC é 2.16.76.1.2.1.11.

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 Subordinada Certisign Múltipla (AC Certisign Múltipla) no âmbito da ICP-Brasil.

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

1.3.2. Autoridades de Registro

1.3.2.1. Os dados a seguir, referentes às Autoridades de Registro – AR utilizadas pela AC Certisign Múltipla 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 Múltipla (<http://www.certisign.com.br/certificacao-digital/repositorios/icp/ac-certisign-multipla>):

- 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 Múltipla, 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 ICPBrasil, se for o caso.

1.3.2.2. A AC Certisign Múltipla 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 Múltipla e/ou por intermédio de suas AR é publicada em serviço de diretório e/ou em página web da AC Certisign Múltipla (<http://icp-brasil.certisign.com.br/repositorio/ac-certisign-multipla/index.htm>).

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

- a) disponibilização de infra-estrutura física e lógica;
- b) disponibilização de recursos humanos especializados; ou

c) disponibilização de infra-estrutura física e lógica e de recursos humanos especializados.

1.3.3.3. A AC Certisign Múltipla mantém as informações acima sempre atualizadas.

1.3.4. Titulares de Certificado

Pessoas físicas ou jurídicas de direito público ou privado, nacionais ou estrangeiras, podem ser titulares de Certificado.

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

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

1.3.5.5. Não se aplica.

1.3.5.6. O “Termo de Titularidade”, no caso de certificados de pessoas jurídicas, disponibilizados pela AR que recebe e valida o pedido de emissão de certificado poderá limitar as aplicações para as quais são adequados os certificados de assinatura – tipo A1 emitidos pela AC Certisign Múltipla, determinando restrições ou proibições de uso destes certificados.

1.4. Dados de Contato

Nome: Certisign Certificadora Digital S.A.

Endereço: Rua do Passeio 70, 7º andar - Centro – Rio de Janeiro - RJ

Telefone: (21) 4501-1800 Fax: (21) 4501-1801

Nome: Anderson Silva de Farias

Telefone: (21) 4501-1840

Fax: (21) 2580-1285

E-mail: icpbrasil@certisign.com.br

2. DISPOSIÇÕES GERAIS

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

2.1.Obrigações e Direitos

2.1.1.Obrigações da AC Certisign Múltipla

2.1.2.Obrigações das AR

2.1.3.Obrigações dos Titulares 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 Múltipla

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 de 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

2.6.2.Freqüência de publicação

2.6.3.Controles de acesso

2.6.4.Repositórios

2.7.Auditoria e Fiscalização

2.8.Sigilo

2.8.1.Tipos de informações sigilosas

2.8.2.Tipos de informações não-sigilosas

2.8.3.Divulgação de informação de revogação ou suspensão de certificado

2.8.4.Quebra de sigilo por motivos legais

2.8.5.Informações a terceiros

2.8.6.Divulgação por solicitação do Titular do Certificado

2.8.7.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 Múltipla.

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 uma organização

3.1.9.Autenticação da identidade do 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 um equipamento ou aplicação

3.1.10.1. Disposições Gerais

3.1.10.2 Procedimentos para efeitos de identificação de um equipamento ou aplicação

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

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

3.3.Geração de novo par de chaves após revogação

3.4.Solicitação de Revogação

4. REQUISITOS OPERACIONAIS

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

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.Freqüência 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.Freqüência 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 de entidade é comprometida

4.8.4.Segurança dos recursos após desastre natural ou de outra natureza

4.8.5.Atividades das Autoridades de Registro

4.9.Extinção dos serviços 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 Múltipla.

5.1. Controles Físicos

5.1.1. Construção e localização das instalações

5.1.2. Acesso físico

5.1.3. Energia e ar condicionado

5.1.4. Exposição à água

5.1.5. Prevenção e proteção contra incêndio

5.1.6. Armazenamento de mídia

5.1.7. Destruição de lixo

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

5.2. Controles Procedimentais

5.2.1. Perfis qualificados

5.2.2. Número de pessoas necessário por tarefa

5.2.3. Identificação e autenticação para cada perfil

5.3. Controles de Pessoal

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

5.3.2. Procedimentos de verificação de antecedentes

5.3.3. Requisitos de treinamento

5.3.4. Freqüência e requisitos para reciclagem técnica

5.3.5. Freqüência e seqüência de rodízio de cargos

5.3.6. Sanções para ações não autorizadas

5.3.7. Requisitos para contratação de pessoal

5.3.8. Documentação fornecida ao pessoal

6. CONTROLES TÉCNICOS DE SEGURANÇA

6.1. Geração e Instalação do Par de Chaves

6.1.1. Geração do par de chaves

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

6.1.1.2. A geração do par de chaves criptográficas ocorre, no mínimo, utilizando CSP (Cryptographic Service Provider) existente na estação do solicitante, apresentados pelo browser Microsoft ou Netscape e, quando da geração, a chave privada é armazenada no HD da estação.

A chave privada poderá ser exportada e armazenada (cópia de segurança) em mídia externa –disquete, token ou cartão inteligente- e protegida por senha de acesso.

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

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

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

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

- a) A chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;
- b) A chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida e 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 Múltipla e descrito nesta PC é o A1.

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, de equipamentos e aplicações.

6.1.2. Entrega da chave privada à entidade titular do certificado

Item não aplicável.

6.1.3. Entrega da chave pública para emissor de certificado

A entrega da chave pública do solicitante do certificado AC Certisign Múltipla, 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 Múltipla 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/ac-certisign-multipla/index.htm>.

6.1.5. Tamanhos de chave

6.1.5.1. O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC Certisign Múltipla é de 1024 bits para as hierarquias V0 e V1 e de 2048 bits para as hierarquias V2 e V3.

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

6.1.6. Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas dos titulares de certificados adotam, no mínimo, o padrão FIPS (Federal Information Processing Standards) 140-1 ou equivalente estabelecido pelo CG da ICP-Brasil.

6.1.7.Verificação da qualidade dos parâmetros

Os parâmetros são verificados de acordo com as normas estabelecidas pelo CMVP (Cryptographic Module Validation Program) do NIST (National Institute of Standards and Technology).

6.1.8.Geração de chave por hardware ou software

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

6.2. Proteção da Chave Privada

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, 140-2 ou outro de conteúdo semelhante a um destes citados.

6.2.2.Controle "n de m" para chave privada

Não se aplica.

6.2.3.Recuperação (escrow) de chave privada

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

6.2.4.Cópia de segurança (backup) de chave privada

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

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

6.2.4.3. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-

Brasil, e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4. O titular do certificado, quando realizar uma cópia de segurança da sua chave privada, deve observar que esta cópia deve ser efetuada com, no mínimo, os mesmos requerimentos de segurança da chave original.

6.2.5.Arquivamento de chave privada

6.2.5.1. A AC Certisign Múltipla não arquivava 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

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

6.2.7.Método de ativação de chave privada

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

6.2.8.Método de desativação de chave privada

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

6.2.9.Método de destruição de chave privada

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

6.3.Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1.Arquivamento de chave pública

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

6.3.2.Períodos de uso para as chaves pública e privada

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

6.3.2.2. Não se aplica.

6.3.2.3. O período máximo de validade admitido para certificados de Assinatura Digital Tipo A1 da AC Certisign Múltipla é de 1 (um) ano.

6.4.Dados de Ativação

6.4.1.Geração e instalação dos dados de ativação

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

6.4.2.Proteção dos dados de ativação

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

6.4.3.Outros aspectos dos dados de ativação

Não se aplica.

6.5.Controles de Segurança Computacional

6.5.1.Requisitos técnicos específicos de segurança computacional

O titular do certificado é responsável pela segurança computacional dos sistemas nos quais são geradas e utilizadas as chaves privadas e deve zelar por sua integridade. O equipamento onde são gerados os pares de chaves criptográficas do titular do Certificado deve dispor de mecanismos mínimos que garantam a segurança computacional, com proteção anti-vírus e criptografia 3DES para a chave privada, armazenada no HD.

6.5.2.Classificação da segurança computacional

Item não aplicável.

6.6. Controles Técnicos do Ciclo de Vida

A AC Certisign Múltipla 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 Múltipla utiliza um modelo clássico espiral no desenvolvimento dos sistemas. 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 Múltipla utiliza uma gerência de configuração, gerência de mudança, testes formais e outros processos informais.

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

6.6.2. Controles de gerenciamento de segurança

6.6.2.1. A AC Certisign Múltipla 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 Múltipla 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

O módulo criptográfico utilizado para armazenamento da chave privada da entidade titular de certificado está em conformidade com o padrão de segurança FIPS 140-1 nível 2 (para a cadeia de certificação V0); ou FIPS 140-2 nível 2 (para a cadeia de certificação V1); ou FIPS 140-2 nível 3 (para cadeia de certificação V2 e V3), utilizando o algoritmo RSA ou ECDSA.

7. PERFIS DE CERTIFICADO E LCR

7.1. Perfil do Certificado

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

7.1.2. Extensões de certificado

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

7.1.2.2. Extensões Obrigatórias

Os certificados emitidos pela AC Certisign Múltipla 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 Múltipla;
- b) **Key Usage**, crítica: somente os bits digitalSignature, nonRepudiation e keyEncipherment estão ativados;
- c) **Certificate Policies**, não crítica contém:
 - O OID desta PC: 2.16.76.1.2.1.11;
 - e o endereço *Web* da DPC AC Certisign Múltipla que emite o certificado: (http://icp-brasil.certisign.com.br/repositorio/dpc/AC_Certisign_Multipla/DPC_AC_CertisignMultipla.pdf).
- d) **CRL Distribution Points**, não crítica: contém os endereços Web onde se obtém a LCR da AC Certisign Múltipla:

Para certificados emitidos até 31/10/2008

[http://icp-](http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisignMultiplaV3/LatestCRL.crl)

[brasil.certisign.com.br/repositorio/lcr/ACCertisignMultiplaV3/LatestCRL.crl](http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisignMultiplaV3/LatestCRL.crl)

[http://icp-](http://icp-brasil.outralcr.com.br/repositorio/lcr/ACCertisignMultiplaV3/LatestCRL.crl)

[brasil.outralcr.com.br/repositorio/lcr/ACCertisignMultiplaV3/LatestCRL.crl](http://icp-brasil.outralcr.com.br/repositorio/lcr/ACCertisignMultiplaV3/LatestCRL.crl)

<http://repositorio.icpbrasil.gov.br/lcr/Certisign/ACCertisignMultiplaV3/LatestCRL.crl>

Para certificados emitidos a partir de 01/11/2008

[http://icp-](http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisignMultiplaG3/LatestCRL.crl)

[brasil.certisign.com.br/repositorio/lcr/ACCertisignMultiplaG3/LatestCRL.crl](http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisignMultiplaG3/LatestCRL.crl)

[http://icp-](http://icp-outralcr.com.br/repositorio/lcr/ACCertisignMultiplaG3/LatestCRL.crl)

[brasil.outralcr.com.br/repositorio/lcr/ACCertisignMultiplaG3/LatestCRL.crl](http://icp-outralcr.com.br/repositorio/lcr/ACCertisignMultiplaG3/LatestCRL.crl)

<http://repositorio.icpbrasil.gov.br/lcr/Certisign/ACCertisignMultiplaG3/LatestCRL.crl>

Para certificados emitidos na G5:

[http://icp-](http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisignMultiplaG5/LatestCRL.crl)

[brasil.certisign.com.br/repositorio/lcr/ACCertisignMultiplaG5/LatestCRL.crl](http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisignMultiplaG5/LatestCRL.crl)

[http://icp-](http://icp-outralcr.com.br/repositorio/lcr/ACCertisignMultiplaG5/LatestCRL.crl)

[brasil.outralcr.com.br/repositorio/lcr/ACCertisignMultiplaG5/LatestCRL.crl](http://icp-outralcr.com.br/repositorio/lcr/ACCertisignMultiplaG5/LatestCRL.crl)

<http://repositorio.icpbrasil.gov.br/lcr/Certisign/ACCertisignMultiplaG5/LatestCRL.crl>

- e) **Authority Information Access**, não crítica: A primeira entrada deve conter o método de acesso id-ad-caIssuer, utilizando um dos seguintes protocolos de acesso, HTTP, HTTPS ou LDAP, para a recuperação da cadeia de certificação. A segunda entrada pode conter o método de acesso id-ad-ocsp, com o respectivo endereço do respondedor OCSP, utilizando um dos seguintes protocolos de acesso, HTTP, HTTPS ou LDAP. Esta extensão somente é aplicável para certificado de usuário final.
- f) **basicConstraints**, não crítica: contém o campo cA=False.

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

a) Para certificado de pessoa física:

a.1) 3 (três) 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 6 (seis) 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 subseqüentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 posições subseqüentes, o município e a UF do Título de Eleitor.

a.2) campos otherName, não obrigatórios, contendo:

i. **rfc822Name**, contém o endereço e-mail do titular do certificado.

ii. · 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) Para certificado de pessoa jurídica:

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

i. OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaa; nas 11 (onze) posições subseqüentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subseqüentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subseqüentes, o número do RG do responsável; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF;

ii. OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado;

iii. OID = 2.16.76.1.3.3 e conteúdo = Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado;

iv. 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.

b.2) campos otherName, não obrigatórios, contendo:

i. **rfc822Name**, contém o endereço e-mail do titular do certificado.

ii. · 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).

c) Para certificado de equipamento ou aplicação:

c.1) 4 (quatro) 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 = 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 ddmmaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do RG do responsável; nas 6 (seis) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

Quando certificados de equipamento forem emitidos para servidores de Domain Controller, adicionalmente irão conter:

c.2) campo otherName, contendo:

OID = 1.3.6.1.4.1.311.25.1 contendo o identificador (Globally Unique Identifier - GUID) do Domain Controller;

c.3) campo **DNS Name**, contendo o nome do domínio.

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

a) O conjunto de informações definido em cada campo otherName é armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING ou PRINTABLE STRING, com exceção do campo UPN que possui uma cadeia de caracteres do tipo ASN.1 UTF8 STRING;

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

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

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

e) As 6 (seis) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, sendo utilizados apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre municípios e UF do Título de Eleitor;

f) Apenas caracteres de A a Z e de 0 a 9 são utilizados, não sendo permitidos caracteres especiais, símbolos, espaços ou quaisquer outros, com exceção do campo UPN que utiliza caracteres especiais;

g) 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 Múltipla, podem ser utilizados com OID atribuídos ou aprovados pela AC-Raiz.

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

7.1.2.7. A AC Certisign Múltipla implementa a extensão "Extended Key Usage", não crítica, contendo o valor "server authentication" (OID 1.3.6.1.5.5.7.3.1), e podendo conter os valores "client authentication" (OID 1.3.6.1.5.5.7.3.2) e/ou "Netscape SGC" (OID 2.16.840.1.113730.4.1) e/ou "Microsoft SGC" (OID 1.3.6.1.4.1.311.10.3.3) para certificados de equipamento, o valor "client authentication" (OID 1.3.6.1.5.5.7.3.2) e podendo conter os valores "code signing" (OID 1.3.6.1.5.5.7.3.3) e/ou "e-mail protection" (id-kp-emailProtection) (OID 1.3.6.1.5.5.7.3.4) e/ou "OCSPSigning" (OID 1.3.6.1.5.5.7.3.9) para certificados de aplicação e 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 podendo conter o valor "Smart Card Logon" (OID 1.3.6.1.4.1.311.20.2.2), quando for utilizado o campo "UPN" na extensão "Subject Alternative Name", para certificados de pessoa jurídica e pessoa física.

7.1.2.8 A AC Certisign Múltipla implementa a extensão Authority Information Access, não crítica, contendo obrigatoriamente o endereço de acesso aos certificados da cadeia de certificação através do link: http://icp-brasil.certisign.com.br/repositorio/certificados/AC_Certisign_Multipla_G5.p7c e opcionalmente o endereço de acesso ao serviço de Consulta On-Line de Situação de Certificado (On-line Certificate Status Protocol- OCSP): <http://ocsp.certisign.com.br>.

7.1.2.9 A AC Certisign Múltipla implementa a extensão Certificate Template Name, não crítica, contendo o valor "DomainController", codificado através da string "BMPString" quando certificados de equipamento forem emitidos para servidores de Domain Controller.

7.1.3. Identificadores de algoritmo

Os certificados emitidos pela AC Certisign Múltipla são assinados com o uso do algoritmo RSA com SHA-1 como função de hash (OID = 1.2.840.113549.1.1.5) nas hierarquias V0 e V1, e 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 V3 conforme o padrão PKCS#1.

7.1.4.Formatos de nome

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

C = BR

O = ICP-Brasil

OU = identificador (indica parâmetro adicional, que pode ser um nome, número, combinação de nome e número ou seqüência alfanumérica)

CN = nome do titular do certificado

E = endereço e-mail do titular do certificado ou do responsável pela pessoa jurídica titular do certificado.

O "Distinguished Name" (DN) pode apresentar até sete campos "OU". Caso qualquer um dos campos OU não seja utilizado, o mesmo terá grafado o texto "(em branco)" ou não será apresentado no DN.

Em um certificado de pessoa jurídica, o identificador CN contém a denominação da razão social correspondente.

Em um certificado de equipamento ou aplicação, o identificador CN contém o URL correspondente ou o nome da aplicação, e não contém o campo E.

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

7.1.5.Restrições de nome

7.1.5.1. As restrições aplicáveis para os nomes dos titulares de certificado emitidos pela AC Certisign Múltipla 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: 2.16.76.1.2.1.11.

Todo certificado emitido segundo essa PC, PC A1 Certisign Múltipla, contém o valor desse OID presente na extensão Certificate Policies.

7.1.7.Uso da extensão "Policy Constraints"

Item não aplicável.

7.1.8.Sintaxe e semântica dos qualificadores de política

Os campos **policyQualifiers** da extensão "*Certificate Policies*" contém o endereço *web* da DPC da AC Certisign Múltipla (http://icp-brasil.certisign.com.br/repositorio/dpc/AC_Certisign_Multipla/DPC_AC_CertiSign_Multipla.pdf).

7.1.9.Semântica de processamento para extensões críticas

Extensões críticas devem ser interpretadas conforme a RFC 5280.

7.2.Perfil de LCR

7.2.1.Número(s) de versão

As LCR geradas pela AC Certisign Múltipla 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 Múltipla e sua criticalidade.

7.2.2.2. As LCR da AC Certisign Múltipla 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 Múltipla.
- b) "CRL Number", não crítica: contém um número seqüencial para cada LCR emitida pela AC Certisign Múltipla.

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 Múltipla. A aprovação e conseqüente adoção de nova versão estarão sujeitas à autorização da AC Raiz.

8.2. Políticas de publicação e notificação

A AC Certisign Múltipla 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/ac-certisign-multipla/index.htm>)

8.3. Procedimentos de aprovação

Esta DPC da AC Certisign Múltipla foi submetida à aprovação, durante o processo de credenciamento da AC Certisign Múltipla, conforme o determinado CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

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 NA ICP-BRASIL	DOC-ICP-01.01
[2]	ATRIBUIÇÃO DE OID NA ICP-BRASIL	DOC-ICP-04.01