

POLÍTICA DE CERTIFICADO
TIPO A3
DA AUTORIDADE CERTIFICADORA BRY
MÚTIPLA

“PC A3 DA AC BRY MÚTIPLA”

Versão 1.1

Junho, 2009

Sumário

SUMÁRIO	2
LISTA DE ACRÔNIMOS	4
1 INTRODUÇÃO	6
1.1 VISÃO GERAL	6
1.2 IDENTIFICAÇÃO	6
1.3 COMUNIDADE E APLICABILIDADE	6
1.4 DADOS DE CONTATO	7
2 DISPOSIÇÕES GERAIS	7
2.1 OBRIGAÇÕES E DIREITOS	7
2.2 RESPONSABILIDADES	7
2.3 RESPONSABILIDADE FINANCEIRA	8
2.4 INTERPRETAÇÃO E EXECUÇÃO	8
2.5 TARIFAS DE SERVIÇO	8
2.6 PUBLICAÇÃO E REPOSITÓRIO	8
2.7 AUDITORIA E FISCALIZAÇÃO	8
2.8 SIGILO	9
2.9 DIREITOS DE PROPRIEDADE INTELECTUAL	9
3 IDENTIFICAÇÃO E AUTENTICAÇÃO	9
3.1 REGISTRO INICIAL	10
3.2 GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL	10
3.3 GERAÇÃO DE NOVO PAR DE CHAVES APÓS REVOGAÇÃO	10
3.4 SOLICITAÇÃO DE REVOGAÇÃO	10
4 REQUISITOS OPERACIONAIS	10
4.1 SOLICITAÇÃO DE CERTIFICADO	11
4.2 EMISSÃO DE CERTIFICADO	11
4.3 ACEITAÇÃO DE CERTIFICADO	11

4.4	SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO	11
4.5	PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA	12
4.6	ARQUIVAMENTO DE REGISTROS.....	12
4.7	TROCA DE CHAVE.....	13
4.8	COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE.....	13
4.9	EXTINÇÃO DOS SERVIÇOS DE AC OU AR	13
5	CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL	13
5.1	CONTROLES FÍSICOS	14
5.2	CONTROLES PROCEDIMENTAIS	14
5.3	CONTROLES DE PESSOAL.....	14
6	CONTROLES TÉCNICOS DE SEGURANÇA.....	15
6.1	GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES.....	15
6.2	PROTEÇÃO DA CHAVE PRIVADA	17
6.3	OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES	18
6.4	DADOS DE ATIVAÇÃO	18
6.5	CONTROLES DE SEGURANÇA COMPUTACIONAL	19
6.6	CONTROLES TÉCNICOS DO CICLO DE VIDA	19
6.7	CONTROLES DE SEGURANÇA DE REDE	20
6.8	CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO.....	20
7	PERFIS DE CERTIFICADO E LCR	20
7.1	PERFIL DO CERTIFICADO	20
7.2	PERFIL DE LCR.....	24
8	ADMINISTRAÇÃO DE ESPECIFICAÇÃO.....	24
8.1	PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO.....	24
8.2	POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO	24
8.3	PROCEDIMENTOS DE APROVAÇÃO	24

LISTA DE ACRÔNIMOS

AC - Autoridade Certificadora

AC BRy - Autoridade Certificadora Raiz da BRy

AC BRy Múltipla - Autoridade Certificadora Múltipla da BRy Tecnologia

AR - Autoridades de Registro

CEI - Cadastro Específico do INSS

CG - Comitê Gestor

CMVP - *Cryptographic Module Validation Program*

CN - *Common Name*

CNPJ - Cadastro Nacional de Pessoas Jurídicas

CPF - Cadastro de Pessoas Físicas

CSP - *Cryptographic Service Provider*

DMZ - Zona Desmilitarizada

DN - *Distinguished Name*

DPC - Declaração de Práticas de Certificação

HD - *Hard disk*

ICP-Brasil - Infra Estrutura de Chaves Públicas Brasileira

ICP-BRY - Infra Estrutura de Chaves Públicas da BRy Tecnologia SA

IDS - Sistemas de Detecção de Intrusão

IEC - *International Electro technical Commission*

ISO - *International Organization for Standardization*

ITU - *International Telecommunications Union*

LCR - Lista de Certificados Revogados

NBR - Norma Brasileira

NIS - Número de Identificação Social

NIST - *National Institute of Standards and Technology*

OCSP - *On-line Certificate Status Protocol*

OID - *Object Identifier*

OU - *Organization Unit*

PASEP - Programa de Formação do Patrimônio do Servidor Público

PC - Política de Certificados

PKCS#1 - *Public Key Cryptography Standard - #1 = RSA Cryptography Standard*

PKCS#7 - *Public Key Cryptography Standard - #7 = Cryptographic Message Syntax Standard*

PKCS#10 - *Public Key Cryptography Standard - #10 = Certification Request Standard*

PIS - Programa de Integração Social

PS - Política de Segurança

PSS - Prestadores de Serviço de Suporte

RFC - *Request for Comments*

RFC 2313: *Internet X.509 Public Key Infrastructure - RSA Encryption*

RFC 2527: *Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework*

RFC 3280: *Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile*

RG - Registro Geral

SNMP - *Simple Network Management Protocol*

SSL - *Secure Socket Layer*

UF - Unidade de Federação

URL - *Uniform Resource Location*

UTC - *Coordinated Universal Time*

1 INTRODUÇÃO

1.1 Visão Geral

Esse documento descreve a Política de Certificados A3 (PC A3) da Autoridade Certificadora da BRy Tecnologia SA. A estrutura desta PC está baseada na RFC 3647 (Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework).

1.2 Identificação

Esta PC é chamada “Política de Certificado de Assinatura Digital Tipo A3 da Autoridade Certificadora BRy Múltipla” e referida como “PC A3 da AC BRy Múltipla”. O OID (*object identifier*) desta PC é 1.3.6.1.4.1.14975.1.3.3.1.

1.3 Comunidade e Aplicabilidade

1.3.1 Autoridades Certificadoras

Esta PC refere-se à AC BRy Múltipla no âmbito da ICP-BRy.

As práticas e procedimentos de certificação estão descritos na Declaração de Práticas de Certificação da AC BRy Múltipla.

1.3.2 Autoridades de Registro

1.3.2.1 Os dados a seguir, referentes às Autoridades de Registro – AR utilizadas pela AC BRy 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 BRy Múltipla (<http://icp.bry.com.br/repositorio>):

- a) relação de todas as AR credenciadas, com informações sobre as PC que implementam.

1.3.3 Titulares de Certificado

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

1.3.4 Aplicabilidade

Os certificados emitidos pela AC BRy Múltipla no âmbito desta PC podem ser utilizados para confirmação de identidade do titular em aplicações como Web, correio eletrônico, transações on-line, redes privadas virtuais, transações eletrônicas, informações eletrônicas; para cifração de chaves de sessão, assinatura de

documentos eletrônicos e verificação da integridade de informações transmitidas eletronicamente. Os certificados também podem ser associados à equipamentos ou aplicações.

O “Termo de Titularidade e Responsabilidade”, no caso de certificados de pessoas jurídicas, poderá limitar as aplicações para as quais são adequados os certificados de assinatura – tipo A3, pela AC BRy Múltipla, determinando restrições ou proibições de uso destes certificados.

1.4 Dados de Contato

Nome: Bry Tecnologia S.A.

Endereço: Rua Lauro Linhares 2123 – Torre B – Sala 306 , Trindade – Florianópolis/SC - CEP: 88036-002

Telefone/FAX: (48) 3234-6696

Nome: Marcelo Luiz Brocardo

E-mail: ac@bry.com.br

2 DISPOSIÇÕES GERAIS

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

2.1 Obrigações e Direitos

2.1.1 Obrigações da AC BRy 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 Múltipla

2.2.2 Responsabilidades da 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

2.6.2 Frequência 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

2.8.8 Direitos de Propriedade Intelectual

2.9 Direitos de Propriedade Intelectual

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

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

3.1 Registro Inicial

3.1.1 Tipos de Nomes

3.1.2 Necessidade de Nomes Significativos

3.1.3 Regras para Interpretação de Vários Tipos de Nomes

3.1.4 Unicidade de Nomes

3.1.5 Procedimento para Resolver Disputa de Nomes

3.1.6 Reconhecimento, Autenticação e Papel de Marcas Registradas

3.1.7 Método para Comprovar a Posse de Chave Privada

3.1.8 Autenticação da Identidade do Indivíduo

3.1.9 Autenticação da Identidade de uma Organização

3.1.10 Autenticidade da Identidade de 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 BRy 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 (*log*)

4.5.3 Período de Retenção para Registros (*log*) 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 ou AR

5 CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Nos itens seguintes são referidos os itens correspondentes da DPC da AC BRy 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

Neste item são descritos: as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos e outros controles técnicos de segurança utilizados pela AC BRy Múltipla e pelas ARs vinculadas na execução de suas funções operacionais.

6.1 Geração e Instalação do Par de Chaves

6.1.1 Geração do Par de Chaves

6.1.1.1. 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. O processo de geração de chaves do tipo A3, contemplada nesta PC, exige:

a) a instalação de hardware e software relacionados à mídia armazenadora do certificado selecionada pelo cliente;

b) o par de chaves será gerado em cartão inteligente ou token, ambos com capacidade de geração de chave, sendo ativados e protegidos por senha e/ou identificação biométrica;

c) o responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado deve executar pessoalmente a geração dos pares de chaves criptográficas.

6.1.1.3. O algoritmo a ser utilizado para a geração das chaves criptográficas de titulares de certificados é o RSA.

6.1.1.4. Ao ser gerada a chave privada do titular do certificado deve ser gravada cifrada, por algoritmo simétrico. 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 A3.

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 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.

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 dispositivo é do titular do certificado, no caso de certificados de pessoa física, e da pessoa responsável, indicada por seus(s) representante(s) legal(s), conforme especificado no Termo de Titularidade e Responsabilidade, no caso de certificados de pessoa jurídica, de equipamentos 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 AC BRy 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 BRy Múltipla disponibiliza o seu certificado, e de todos os certificados da cadeia de certificação, para os usuários, através de endereço Web: <http://icp.bry.com.br/repositorio>.

6.1.5 Tamanhos de Chave

6.1.5.1. O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC BRy Múltipla é de 1024 bits.

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.

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 dos certificados previstos nesta PC é realizada por *hardware* criptográfico.

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

Os certificados têm ativado os bits: *digitalSignature*, *nonRepudiation* e *keyEncipherment*.

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 Custódia (*escrow*) de Chave Privada

Não é permitida, no âmbito da ICP-BRy, a recuperação (*escrow*) de chaves privadas de assinatura, isto é, não se permite que terceiros possam obter uma chave privada de assinatura.

6.2.4 Cópia de Segurança (*backup*) de Chave Privada

Qualquer entidade titular de certificado pode, a seu critério, manter cópia de segurança de sua chave privada. 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 BRy Múltipla não guarda 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 poderá definir procedimentos necessários para 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 BRy Múltipla permanecem armazenadas após a expiração dos certificados correspondentes, por no mínimo 30 (trinta) anos, 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 BRy 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. O período máximo de validade admitido para certificados de Assinatura Digital Tipo A3 da AC BRy Múltipla é de 3 (três) anos.

6.4 Dados de Ativação

6.4.1 Geração e Instalação dos Dados de Ativação

Os certificados de tipo A3 se utilizam, para geração e armazenamento do par de chaves e certificado, de cartão inteligente ou token, ambos com capacidade de geração de chave, sendo ativados e protegidos por senha e/ou identificação biométrica.

No caso de ativação por senha, recomenda-se que as mesmas sejam criadas de forma aleatória, respeitando-se procedimentos básicos de segurança, tais como:

- a) nunca fornecer senha a terceiros;
- b) escolher senhas de 8 ou mais caracteres;
- c) definir senhas com caracteres numéricos e alfanuméricos;
- d) memorizar a senha e
- e) não escrevê-la.

6.4.2 Proteção dos Dados de Ativação

Para a proteção dos dados de ativação da chave privada da entidade titular do certificado, no caso de ativação por senha, recomenda-se:

- f) nunca fornecer senha a terceiros;
- g) escolher senhas de 8 ou mais caracteres;
- h) definir senhas com caracteres numéricos e alfanuméricos;
- i) memorizar a senha e
- j) não escrevê-la.

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 dispositivo 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 simétrica para a chave privada, armazenada no HD.

6.5.2 Classificação da Segurança Computacional

Não se aplica.

6.6 Controles Técnicos do Ciclo de Vida

Não se aplica.

6.6.1 Controles de Desenvolvimento de Sistema

Não se aplica.

6.6.2 Controles de Gerenciamento de Segurança

Não se aplica.

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

Conforme os itens 6.2.6.

7 PERFIS DE CERTIFICADO E LCR

7.1 Perfil do Certificado

Todos os certificados emitidos pela AC BRy 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 BRy Múltipla implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 3280.

7.1.2 Extensões de Certificado

Os certificados emitidos pela AC BRy MÚLTIPLA para usuários finais contêm as seguintes extensões:

- **basicConstraints**, crítica: deve conter o campo *cA=False*;
- **keyUsage**, crítica: somente os bits
 - o **Tipo A3**: *digitalSignature*, *nonRepudiation* e *keyEncipherment* estão ativados;
- **cRLDistributionPoints**, não crítica: contém o endereço da página *web* (http://icp.bry.com.br/repositorio/lcr/ac_bry_multipla.crl) onde se obtém a LCR da AC BRy Múltipla;
- **Certificate Policies**, não crítica: o campo *policyIdentifier* contém o OID da PC que implementa e o campo *policyQualifiers* contém o endereço da página *web* (http://icp.bry.com.br/repositorio/pc/pc_a3_ac_bry_multipla.pdf) onde está a DPC da AC BRy Múltipla;
- **Authority Key Identifier**, não crítica: o campo *keyIdentifier* contém o hash SHA-1 da chave pública da AC BRy Múltipla.

A AC BRy Múltipla implementa a extensão "Extended Key Usage", não crítica, contendo os valores "server authentication" (OID 1.3.6.1.5.5.7.3.1) e "client authentication" (OID 1.3.6.1.5.5.7.3.2) para certificados de equipamento e os valores "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) para certificados de pessoa jurídica e de pessoa física.

Os certificados emitidos para usuário final possuem a extensão **Subject Alternative Name**, não crítica e com os seguintes formatos:

Para certificado de pessoa física, 3 (três) campos **otherName**, contendo, nesta ordem:
'PC A3 da AC BRy Múltipla v1.1

1. OID = 2.16.76.1.3.1 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato ddmmaaaa; nas 11 (onze) posições subseqüentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subseqüentes, o Número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subseqüentes, o número do Registro Geral (RG) do titular; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva unidade da federação;
2. 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;
3. OID = 2.16.76.1.3.5 e conteúdo nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subseqüentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 posições subseqüentes, o município e a UF do Título de Eleitor, rfc822Name, extensão **Subject Alternative Name**, contém o endereço e-mail do titular do certificado.

Para certificado de pessoa jurídica, 4 (quatro) campos **otherName**, contendo, nesta ordem:

1. OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições subseqüentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subseqüentes, o Número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subseqüentes, o número do Registro Geral (RG) do responsável; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva unidade da federação;
2. OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado;
3. OID = 2.16.76.1.3.3 e conteúdo = Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica do titular do certificado;
4. 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; rfc822Name, extensão **Subject Alternative Name**, contém o endereço e-mail do responsável pela pessoa jurídica titular do certificado.

Para certificado de equipamentos ou aplicações, 4 (quatro) campos **otherName**, contendo, nesta ordem:

1. OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições subseqüentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subseqüentes, o Número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subseqüentes, o número do Registro Geral (RG) do responsável; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva unidade da federação;
2. OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado;
3. OID = 2.16.76.1.3.3 e conteúdo = Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado;
4. 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.

O conjunto de informações definido em cada campo **otherName** é armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING.

Quando os números de CPF, NIS (PIS, PASEP ou CI), RG, CNPJ, CEI ou Título de Eleitor não estiverem disponíveis, os campos correspondentes são integralmente preenchidos com caracteres “zero”.

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.

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.

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.

Apenas caracteres de A a Z e de 0 a 9 são utilizados, não sendo permitidos caracteres especiais, símbolos, espaços ou quaisquer outros.

Campos **otherName** adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidos, podem ser utilizados com OID atribuídos ou aprovados pela ICP-BRY.

Os outros campos que compõem a extensão **Subject Alternative Name** podem ser utilizados, na forma e com os propósitos definidos na RFC 3280.

7.1.3 Identificadores de Algoritmo

Os certificados emitidos são assinados com o uso do algoritmo RSA com SHA-1 como função de *hash* (OID = 1.2.840.113549.1.1.5), 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 (país) = BR

S (estado) = <Estado do titular>

O (ORGANIZAÇÃO) = **BRY TECNOLOGIA S.A.**

L (cidade) = <Cidade do titular>

OU = **AUTORIDADE CERTIFICADORA**

CN = <nome do titular do certificado>

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

Caso o campo OU acima não seja utilizado, o mesmo terá grafado o texto "(EM BRANCO)".

Em um certificado de pessoa jurídica, o identificador CN contém o nome empresarial constante do CNPJ.

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

O nome é escrito até o limite do campo disponível é vetada abreviatura.

7.1.5 Restrições de Nome

As restrições aplicáveis para os nomes dos titulares de certificado emitidos são as seguintes:

- não são admitidos sinais de acentuação, trema ou cedilhas;
- além dos caracteres alfanuméricos, poderão ser utilizados somente os seguintes caracteres especiais:

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

7.1.6 OID (*Object Identifier*) de Política de Certificado

O OID desta PC é: 1.3.6.1.4.1.14975.1.3.3.1.

7.1.7 Uso da Extensão Policy Constraints

Não se aplica.

7.1.8 Sintaxe e Semântica dos Qualificadores de Política

7.1.9 Semântica de Processamento para Extensões Críticas

Extensões críticas devem ser interpretadas conforme a RFC 3280.

7.2 Perfil de LCR

7.2.1 Número(s) de Versão

A Lista de Certificados Revogados gerada pela AC BRy Múltipla implementa a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 3280.

7.2.2 Extensões de LCR e de Suas Entradas

As seguintes extensões de LCR geradas pela AC BRy Múltipla:

- **AuthorityKeyIdentifier**: contém o resumo SHA-1 da chave pública da AC BRy Múltipla;
- **cRLNumber**, não crítica: contém número seqüencial para cada LCR emitida.

8 ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1 Procedimentos de Mudança de Especificação

Qualquer alteração nesta PC deverá ser submetida para aprovação do CG da ICP-BRy.

8.2 Políticas de Publicação e Notificação

Esta PC está publicada na página *web* da ICP-BRy:

http://icp.bry.com.br/repositorio/pc/pc_a3_ac_bry_multipla.pdf.

8.3 Procedimentos de Aprovação

Os procedimentos de aprovação deste documento são estabelecidos à critério do CG da ICP-BRy.