

**Política de Certificado A3
da Autoridade Certificadora
ONLINE BRASIL
(PC A3 da AC ONLINE BRASIL)**

**OID: 2.16.76.1.2.3.45
Versão 1.1 de 04.08.2015**

Conteúdo

1. INTRODUÇÃO	10
1.1. VISÃO GERAL	10
1.2. IDENTIFICAÇÃO	10
1.3. COMUNIDADE E APLICABILIDADE	10
1.3.1. Autoridades Certificadoras	10
1.3.2. Autoridades De Registro	11
1.3.3 Prestador de Serviço de Suporte	11
1.3.4. Titulares de Certificado	12
1.3.5. Aplicabilidade	12
1.4. DADOS DE CONTATO	13
1.4.1. Pessoas de Contato	13
2. DISPOSIÇÕES GERAIS	13
2.1. OBRIGAÇÕES E DIREITOS	13
2.1.1. Obrigações da AC	13
2.1.2. Obrigações das ARs	13
2.1.3. Obrigações do Titular do Certificado	13
2.1.4. Direitos da terceira parte (<i>Relying Party</i>)	13
2.1.5. Obrigações do Repositório	13
2.2. RESPONSABILIDADES	14
2.2.1. Responsabilidades da AC	14
2.2.2. Responsabilidades da AR	14
2.3. RESPONSABILIDADE FINANCEIRA	14
2.3.1. Indenizações devidas pela terceira parte (<i>Relying Party</i>)	14
2.3.2. Relações Fiduciárias	14
2.3.3. Processos Administrativos	14
2.4. INTERPRETAÇÃO E EXECUÇÃO	14
2.4.1. Legislação	14
2.4.2. Forma de interpretação e notificação	14
2.4.3. Procedimentos de solução de disputa	14
2.5. TARIFAS DE SERVIÇO	14
2.5.1. Tarifas de emissão e renovação de certificados	14
2.5.2. Tarifas de acesso a certificados	14

2.5.3. Tarifas de revogação ou de acesso à informação de status.....	14
2.5.4. Tarifas para outros serviços.....	14
2.5.5. Política de reembolso.....	14
2.6. PUBLICAÇÃO E REPOSITÓRIO.....	14
2.6.1. Publicação de informação da AC.....	14
2.6.2. Frequência de publicação.....	14
2.6.3. Controles de acesso.....	14
2.6.4. Repositórios.....	14
2.7. AUDITORIA E FISCALIZAÇÃO.....	14
2.8. SIGILO.....	14
2.8.1. Tipos de informações sigilosas.....	14
2.8.2. Tipos de informações não sigilosas.....	15
2.8.3. Divulgação de informação de revogação e de suspensão de certificado.....	15
2.8.4. Quebra de sigilo por motivos legais.....	15
2.8.5. Informações a terceiros.....	15
2.8.6. Divulgação por solicitação do titular.....	15
2.8.7. Outras circunstâncias de divulgação de informação.....	15
2.9. DIREITOS DE PROPRIEDADE INTELECTUAL.....	15
3. IDENTIFICAÇÃO E AUTENTICAÇÃO.....	15
3.1. REGISTRO INICIAL.....	15
3.1.1. Disposições Gerais.....	15
3.1.2. Tipos de nomes.....	15
3.1.3. Necessidade de nomes significativos.....	15
3.1.4. Regras para interpretação de vários tipos de nomes.....	15
3.1.5. Unicidade de nomes.....	15
3.1.6. Procedimento para resolver disputa de nomes.....	15
3.1.7. Reconhecimento, autenticação e papel de marcas registradas.....	15
3.1.8. Método para comprovar a posse de chave privada.....	15
3.1.9. Autenticação da identidade de um indivíduo.....	15
3.1.9.1. Documentos para efeitos de identificação de um indivíduo.....	15
3.1.9.2. Informações contidas no certificado emitido para um indivíduo.....	15
3.1.10. Autenticação da identidade de uma organização.....	15
3.1.11. Autenticação da identidade de equipamento ou aplicação.....	15
3.2. GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL.....	15

3.3. GERAÇÃO DE NOVO PAR DE CHAVES APÓS EXPIRAÇÃO OU REVOGAÇÃO	15
3.4. SOLICITAÇÃO DE REVOGAÇÃO	16
4. REQUISITOS OPERACIONAIS	16
4.1. SOLICITAÇÃO DE CERTIFICADO	16
4.2. EMISSÃO DE CERTIFICADO	16
4.3. ACEITAÇÃO DE CERTIFICADO	16
4.4. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO	16
4.4.1. Circunstâncias para revogação	16
4.4.2. Quem pode solicitar revogação	16
4.4.3. Procedimento para solicitação de revogação	16
4.4.4. Prazo para solicitação de revogação	16
4.4.5. Circunstâncias para suspensão	16
4.4.6. Quem pode solicitar suspensão	16
4.4.7. Procedimento para solicitação de suspensão	16
4.4.8. Limites no período de suspensão	16
4.4.9. Frequência de emissão de LCR	16
4.4.10. Requisitos para verificação de LCR	16
4.4.11. Disponibilidade para revogação ou verificação de status on-line	16
4.4.12. Requisitos para verificação de revogação on-line	16
4.4.13. Outras formas disponíveis para divulgação de revogação	16
4.4.14. Requisitos para verificação de outras formas de divulgação de revogação	16
4.4.15. Requisitos especiais para o caso de comprometimento de chave	16
4.5. PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA	16
4.5.1. Tipos de eventos registrados	16
4.5.2. Frequência de auditoria de registros (logs)	17
4.5.3. Período de retenção para registros (logs) de auditoria	17
4.5.4. Proteção de registro (log) de auditoria	17
4.5.5. Procedimentos para cópia de segurança (backup) de registro (log) de auditoria	17
4.5.6. Sistema de coleta de dados de auditoria	17
4.5.7. Notificação de agentes causadores de eventos	17
4.5.8. Avaliações de vulnerabilidade	17
4.6. ARQUIVAMENTO DE REGISTROS	17
4.6.1. Tipos de registros arquivados	17
4.6.2. Período de retenção para arquivo	17

4.6.3. Proteção de arquivo.....	17
4.6.4. Procedimentos para cópia de segurança (backup) de arquivo.....	17
4.6.5. Requisitos para datação (time-stamping) de registros.....	17
4.6.6. Sistema de coleta de dados de arquivo.....	17
4.6.7. Procedimentos para obter e verificar informação de arquivo.....	17
4.7. TROCA DE CHAVE.....	17
4.8. COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE.....	17
4.8.1. Recursos computacionais, software ou dados são corrompidos.....	17
4.8.2. Certificado de entidade é revogado.....	17
4.8.3. Chave de entidade é comprometida.....	17
4.8.4. Segurança dos recursos após desastre natural ou de outra natureza.....	17
4.8.5. Atividades das Autoridades de Registro.....	17
4.9. EXTINÇÃO DOS SERVIÇOS DE AC, AR OU PSS.....	17
5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL.....	17
5.1. CONTROLES FÍSICOS.....	18
5.1.1. Construção e localização das instalações.....	18
5.1.2. Acesso físico.....	18
5.1.3. Energia e ar condicionado.....	18
5.1.4. Exposição à água.....	18
5.1.5. Prevenção e proteção contra incêndio.....	18
5.1.6. Armazenamento de mídia.....	18
5.1.7. Destruição de lixo.....	18
5.1.8. Instalações de segurança (backup) externas (off-site).....	18
5.2. CONTROLES PROCEDIMENTAIS.....	18
5.2.1. Perfis qualificados.....	18
5.2.2. Número de pessoas necessário por tarefa.....	18
5.2.3. Identificação e autenticação para cada perfil.....	18
5.3. CONTROLES DE PESSOAL.....	18
5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade.....	18
5.3.2. Procedimentos de verificação de antecedentes.....	18
5.3.3. Requisitos de treinamento.....	18
5.3.4. Frequência e requisitos para reciclagem técnica.....	18
5.3.5. Frequência e sequência de rodízio de cargos.....	18
5.3.6. Sanções para ações não autorizadas.....	18
5.3.7. Requisitos para contratação de pessoal.....	18
5.3.8. Documentação fornecida ao pessoal.....	18

6. CONTROLES TÉCNICOS DE SEGURANÇA	18
6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES	19
6.1.1. Geração do par de chaves	19
6.1.2. Entrega da chave privada à entidade titular	20
6.1.3. Entrega da chave pública para o emissor de certificado	20
6.1.4. Disponibilização de chave pública da AC para usuários	20
6.1.5. Tamanhos de chave	20
6.1.6 Geração de parâmetros de chaves assimétricas	20
6.1.7 Verificação da qualidade dos parâmetros	20
6.1.8 Geração de chave por hardware ou software	21
6.1.9. Propósitos de uso de chave (conforme o campo “key usage” na X.509 v3)	21
6.2. PROTEÇÃO DA CHAVE PRIVADA	21
6.2.1. Padrões para módulo criptográfico	21
6.2.2. Controle “n de m” para chave privada	21
6.2.3. Custódia (<i>escrow</i>) de chave privada	21
6.2.4. Cópia de segurança (<i>backup</i>) de chave privada	21
6.2.5 Arquivamento de chave privada	22
6.2.6 Inserção de chave privada em módulo criptográfico	22
6.2.7. Método de ativação de chave privada	22
6.2.8. Método de desativação de chave privada	22
6.2.9 Método de destruição de chave privada	22
6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES	22
6.3.1 Arquivamento de chave pública	22
6.3.2 Períodos de uso para as chaves pública e privada	22
6.4 DADOS DE ATIVAÇÃO	23
6.4.1 Geração e instalação dos dados de ativação	23
6.4.2 Proteção dos dados de ativação	23
6.4.3 Outros aspectos dos dados de ativação	23
6.5 CONTROLES DE SEGURANÇA COMPUTACIONAL	23
6.5.1 Requisitos técnicos específicos de segurança computacional	23
6.5.2 Classificação da segurança computacional	24
6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA	24
6.6.1. Controles de desenvolvimento de sistema	24
6.6.2 Controles de gerenciamento de segurança	24
6.6.3 Classificações de segurança de ciclo de vida	24
6.6.4 Controles na geração da LCR antes de publicadas	24

6.7. CONTROLES DE SEGURANÇA DE REDE	24
6.8 CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO	24
7. PERFIS DE CERTIFICADO E LCR	24
7.1 PERFIL DO CERTIFICADO	25
7.1.1 Número de versão	25
7.1.2 Extensões de certificado	25
7.1.4 FORMATOS DE NOME	31
7.1.5. Restrições de nome	32
7.1.6 OID (Object Identifier) de Política de Certificado	33
7.1.7 Uso da extensão “Policy Constraints”	33
7.1.8 Sintaxe e semântica dos qualificadores de política	33
7.1.9. Semântica de processamento para extensões críticas	33
7.2. PERFIL DE LCR	33
7.2.1. Número de versão	33
7.2.2 Extensões de LCR e de suas entradas	33
8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO	34
8.1. PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO	34
8.2. POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO	34
8.3 PROCEDIMENTOS DE APROVAÇÃO	34
9. DOCUMENTOS REFERENCIADOS	34

LISTA DE ACRÔNIMOS

AC - Autoridade Certificadora

AC Raiz - Autoridade Certificadora Raiz da ICP-Brasil

AR - Autoridades de Registro

CEI - Cadastro Específico do INSS

CG - Comitê Gestor

CMM-SEI - Capability Maturity Model do *Software* Engineering Institute

CMVP - Cryptographic Module Validation Program

CN - Common Name

CNE - Carteira Nacional de Estrangeiro

CNPJ - Cadastro Nacional de Pessoas Jurídicas

COBIT - Control Objectives for Information and related Technology

COSO - Comitee of Sponsoring Organizations

CPF - Cadastro de Pessoas Físicas

DMZ - Zona Desmilitarizada

DN - Distinguished Name



DPC - Declaração de Práticas de Certificação

ICP-Brasil - Infraestrutura de Chaves Públicas Brasileira

IDS - Sistemas de Detecção de Intrusão

IEC - International Electrotechnical Commission

ISO – International Organization for Standardization

ITSEC - European Information Technology Security Evaluation Criteria

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 - *Online* Certificate Status Protocol

OID - Object Identifier

OU - Organization Unit

PASEP - Programa de Formação do Patrimônio do Servidor Público

PC - Políticas de Certificado

PCN - Plano de Continuidade de Negócio

PIS - Programa de Integração Social

POP - Proof of Possession

PSS - Prestadores de Serviço de Suporte

RFC – Request For Comments

RG - Registro Geral

SNMP - Simple Network Management Protocol

TCSEC - Trusted System Evaluation Criteria



TSDM - Trusted *Software* Development Methodology

UF - Unidade de Federação

URL - Uniform Resource Location

1. INTRODUÇÃO

1.1. VISÃO GERAL

1.1.1 Esta Política de Certificados (PC) descreve as características e as utilizações dos certificados de Assinatura Digital do tipo A3, emitidos pela Autoridade Certificadora AC ONLINE BRASIL, integrante da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

1.1.2 A estrutura desta PC está baseada no documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL (DOC-ICP-04).

1.1.3 O tipo de certificado emitido sob esta PC é o Tipo A3.

1.1.4 Item não aplicável.

1.1.5 Item não aplicável.

1.1.6 Item não aplicável.

1.1.7 Item não aplicável.

1.2. IDENTIFICAÇÃO

1.2.1 Esta PC é chamada “Política de Certificado de Assinatura Digital Tipo A3 da Autoridade Certificadora ONLINE BRASIL” e referida como “PC A3 da AC ONLINE BRASIL”. O Object Identifier (OID) atribuído para esta PC, após processo de credenciamento da AC junto à ICP-Brasil, é: **2.16.76.1.2.3.45**.

1.2.2 Item não aplicável.

1.3. COMUNIDADE E APLICABILIDADE

1.3.1. Autoridades Certificadoras

1.3.1.1 Esta PC é implementada pela Autoridade Certificadora AC ONLINE BRASIL, integrante da Infraestrutura de Chaves Públicas Brasileira, ICP-Brasil, sob a hierarquia da Autoridade Certificadora VALID, que por sua vez está subordinada hierarquicamente à Autoridade Certificadora Raiz Brasileira.

1.3.1.2 As práticas e procedimentos de certificação utilizados pela AC ONLINE BRASIL estão descritas em sua Declaração de Práticas de Certificação (DPC da AC ONLINE BRASIL), que se encontra publicada no seu repositório, no seguinte endereço:

<http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil/dpc-ac-onlinebrasil.pdf>

1.3.2. Autoridades De Registro

1.3.2.1 A AC ONLINE BRASIL mantém página web <http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil-inf/> onde estão publicados os seguintes dados, referentes às Autoridades de Registro (ARs) que realizam os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes:

- a) relação de todas as ARs 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 ARs que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento;
- e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectiva data de encerramento das atividades;
- f) acordos operacionais celebrados pelas ARs vinculadas com outras ARs da ICP-Brasil, se for caso.

1.3.2.2. A AC ONLINE BRASIL mantém as informações acima sempre atualizadas.

1.3.3 Prestador de Serviço de Suporte

1.3.3.1 A AC ONLINE BRASIL utiliza os seguintes Prestadores de Serviço de Suporte (PSS) nas suas operações:

- a) VALID CERTIFICADORA DIGITAL LTDA.
- b) VALID SOLUÇÕES E SERVIÇOS DE SEGURANÇA EM MEIOS DE PAGAMENTO E IDENTIFICAÇÃO S.A.

1.3.3.2 PSS são entidades utilizadas pela AC ou pela AR para desempenhar as atividades descritas abaixo:

- 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 ONLINE BRASIL mantém as informações sobre seus PSS atualizadas em seu repositório.

1.3.4. Titulares de Certificado

Podem ser titulares de certificados emitidos segundo esta PC pessoas físicas ou jurídicas de direito público ou privado, nacionais ou estrangeiras.

1.3.5. Aplicabilidade

1.3.5.1. Neste item são relacionadas às 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 ONLINE BRASIL 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 ONLINE BRASIL no âmbito desta PC podem ser utilizados em aplicações como:

- Assinatura digital em correio eletrônico;
- Assinatura de código de software;
- Acesso a aplicações disponibilizadas pela Receita Federal do Brasil ou por qualquer outro órgão da Administração Pública Direta ou Indireta que aceite esse certificado;
- Assinatura digital de documentos utilizando software de assinatura elaborado por órgãos, entidades ou empresas diversas;
- Confirmação de identidade na Web;
- Transações eletrônicas e transações on-line;
- Redes privadas virtuais (VPN);
- Cifração de chaves de sessão;
- Autenticação de servidores e equipamentos utilizando protocolos seguros (SSL, TLS, etc.).

1.3.5.5. Não se aplica.

1.3.5.6. Não se aplica

1.3.5.7 No caso de certificados de pessoas jurídicas, o “Termo de Titularidade”, poderá limitar as aplicações para as quais são adequados os certificados de assinatura tipo A3 emitidos pela AC ONLINE BRASIL, determinando restrições ou proibições de uso destes certificados.

1.3.5.8 Para os certificados de Aplicação, são considerados os propósitos de: Assinatura, E-mail Seguro, OCSP. Os propósitos do certificado de aplicação são excludentes, o certificado utilizado para um propósito não poderá ser utilizado cumulativamente para outro.

1.4. DADOS DE CONTATO

Esta PC é administrada pela ONLINE CERTIFICADORA LTDA - ME

Endereço: Av. Miguel Sutil, 8.388 – Salas 604, 605, 608 e 609 – Ed. Avantgarde Business.

CEP: 78040-365

Telefone: (65)2121-0886

Página Web: www.onlinecertificadora.com.br

E-mail: aconline@onlinecertificadora.com.br

Pessoas de Contato

Nome: Júlio Cesar Moraes e Souza

E-mail: julio.souza@onlinecertificadora.com.br

Telefone: (65) 2121-0886

2. DISPOSIÇÕES GERAIS

Os itens seguintes estão descritos da DPC AC ONLINE BRASIL.

2.1. OBRIGAÇÕES E DIREITOS

2.1.1. Obrigações da AC

2.1.2. Obrigações das ARs

2.1.3. Obrigações do Titular do Certificado

2.1.4. Direitos da terceira parte (*Relying Party*)

2.1.5. Obrigações do Repositório

2.2. RESPONSABILIDADES

2.2.1. Responsabilidades da AC

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 a certificados

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. 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 e de 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

2.8.7. Outras circunstâncias de divulgação de informação

2.9. DIREITOS DE PROPRIEDADE INTELECTUAL

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

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

3.1.11. Autenticação 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 EXPIRAÇÃO OU REVOGAÇÃO

3.4. SOLICITAÇÃO DE REVOGAÇÃO

4. REQUISITOS OPERACIONAIS

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 ou dados são 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

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. Frequência e requisitos para reciclagem técnica

5.3.5. Frequência e sequência 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

Nos itens seguintes são definidas as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo esta PC A3 da AC ONLINE BRASIL. São definidos também outros controles técnicos de segurança utilizados pela AC ONLINE BRASIL 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 Quando o titular de certificado for uma pessoa física, esta será a responsável pela geração dos pares de chaves criptográficas. 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.

6.1.1.2 A geração do par de chaves criptográficas ocorre utilizando cartão inteligente ou token, ambos com capacidade de geração de chave e 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 da entidade titular é gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

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

6.1.1.6 A mídia de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) a chave privada é única e seu sigilo é suficientemente assegurado;

b) a chave privada não pode, com uma segurança razoável, ser deduzida e deve estar protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;
e

c) a chave privada pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

6.1.1.7 Essa mídia de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura. O tipo de certificado emitido pela AC ONLINE BRASIL e descrito nesta PC é o A3.

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

6.1.2. Entrega da chave privada à entidade titular

Item não aplicável.

6.1.3. Entrega da chave pública para o emissor de certificado

Chaves públicas são entregues à AC ONLINE BRASIL por meio de uma troca *on-line* utilizando funções automáticas do *software* de certificação da AC ONLINE BRASIL. A mensagem de solicitação de certificado obedece ao formato PKCS#10, que inclui, na própria mensagem, a assinatura digital, realizada com a chave privada correspondente à chave pública contida na solicitação.

6.1.4. Disponibilização de chave pública da AC para usuários

As formas para a disponibilização dos certificados da cadeia de certificação, para os usuários da AC ONLINE BRASIL compreendem:

- a) no momento da disponibilização de um certificado para seu titular, será utilizado o formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1];
- b) página *web* da AC ONLINE BRASIL www.onlinecertificadora.com.br
- c) outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

6.1.5.1 Os certificados emitidos de acordo com esta PC situam-se sob a cadeia da Autoridade Certificadora Raiz Brasileira V2. O tamanho das chaves criptográficas associadas é de 2048 bits.

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

6.1.6 Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas dos titulares de 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 no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.8 Geração de chave por hardware ou software

O processo de geração do par de chaves dos Titulares do Certificado é feito por *hardware*.

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

As chaves privadas dos Titulares de Certificados emitidos pela AC ONLINE BRASIL serão utilizadas para as aplicações descritas no item 1.3.5. Para tanto, os certificados têm ativados os bits digitalSignature, nonRepudiation e keyEncipherment.

6.2. PROTEÇÃO DA CHAVE PRIVADA

Neste item são definidos os requisitos de proteção das chaves privadas de certificados emitidos, segundo a PC A3 da AC ONLINE BRASIL.

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

citados conforme definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.2.2. Controle “n de m” para chave privada

Item não aplicável.

6.2.3. Custódia (*escrow*) de chave privada

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

6.2.4. Cópia de segurança (*backup*) de chave privada

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

6.2.4.2 A AC ONLINE BRASIL responsável por esta PC não mantém cópia de segurança de chave privada de titular.

6.2.4.3 A cópia de segurança deverá ser armazenada cifrada por algoritmo simétrico aprovado pelo documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [1] e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4 Não se aplica.

6.2.5 Arquivamento de chave privada

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

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

6.2.6 Inserção de chave privada em módulo criptográfico

Não se aplica.

6.2.7. Método de ativação de chave privada

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

6.2.8. Método de desativação de chave privada

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

6.2.9 Método de destruição de chave privada

O titular do 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 da AC ONLINE BRASIL, de titulares dos certificados de assinatura digital e as *LCRs* emitidas pela AC ONLINE BRASIL são armazenadas permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2 Períodos de uso para as chaves pública e privada

6.3.2.1 As chaves privadas dos respectivos Titulares são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas poderão ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2 Não se aplica.

6.3.2.3 Certificados do tipo A3 previstos nesta PC têm validade de até **5 anos**.

6.4 DADOS DE ATIVAÇÃO

6.4.1 Geração e instalação dos dados de ativação

Para certificados de tipo A3, a geração e armazenamento do par de chaves são realizados em cartão inteligente ou token, ambos com capacidade de geração de chave, sendo ativados e protegidos por senha.

6.4.2 Proteção dos dados de ativação

Recomenda-se que as senhas de ativação 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.

6.4.3 Outros aspectos dos dados de ativação

Item não aplicável.

6.5 CONTROLES DE SEGURANÇA COMPUTACIONAL

6.5.1 Requisitos técnicos específicos de segurança computacional

Recomenda-se que os equipamentos onde são geradas e utilizadas as chaves privadas disponham de mecanismos mínimos de segurança computacional, tais como:

- a) Senha de bios ativada;
- b) Controle de acesso lógico ao sistema operacional;
- c) Exigência de uso de senhas fortes;
- d) Diretivas de senha e de bloqueio de conta;
- e) Antivírus, antitrojan e antispysware, instalados, atualizados e habilitados;
- f) Firewall pessoal ou corporativo ativado, com permissões de acesso mínimas necessárias às atividades;
- g) Sistema operacional mantido atualizado, com aplicação de correções necessárias (patches, hotfix, etc.);
- h) Proteção de tela acionada no máximo após cinco minutos de inatividade e exigindo senha do usuário para desbloqueio.

6.5.2 Classificação da segurança computacional

Item não aplicável.

6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA

Item não aplicável.

6.6.1. Controles de desenvolvimento de sistema

Item não aplicável.

6.6.2 Controles de gerenciamento de segurança

Item não aplicável.

6.6.3 Classificações de segurança de ciclo de vida

Item não aplicável.

6.6.4 Controles na geração da LCR antes de publicadas

Item não aplicável.

6.7. CONTROLES DE SEGURANÇA DE REDE

Item não aplicável.

6.8 CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO

AC ONLINE BRASIL adota o padrão de Homologação da ICP-Brasil NSH-2, conforme os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

7. PERFIS DE CERTIFICADO E LCR

Os itens seguintes especificam os formatos dos certificados e das *LCRs* gerados segundo esta PC. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões.

7.1 PERFIL DO CERTIFICADO

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

7.1.1 Número de versão

Todos os certificados emitidos pela AC ONLINE BRASIL, segundo esta PC, implementam a versão 3 de certificado definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2 Extensões de certificado

7.1.2.1. Neste item, a PC descreve todas as extensões de certificados utilizadas e sua criticidade.

7.1.2.2. A AC ONLINE BRASIL implementa nos certificados emitidos segundo esta PC as seguintes extensões, definidas como obrigatórias pela ICP-Brasil:

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

b) “**Key Usage**”, **crítica**: somente os bits `digitalSignature`, `nonRepudiation` e `keyEncipherment` são ativados;

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

c.1) o campo `policyIdentifier` contém o OID: 2.16.76.1.2.3.45 desta PC;

c.2) o campo `PolicyQualifiers` contém o endereço *Web* onde se obtém a DPC da AC ONLINE BRASIL:

<http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil/dpc-ac-onlinebrasil.pdf>

d) “**CRL Distribution Points**”, **não crítica**: contém o endereço *URL* das páginas *Web* onde se obtém a LCR da AC ONLINE BRASIL;

d1) <http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil/lcr-ac-onlinebrasilv2.crl>

d2) <http://icp-brasil2.validcertificadora.com.br/ac-onlinebrasil/lcr-ac-onlinebrasilv2.crl>

d3) <http://repositorio.icpbrasil.gov.br/lcr/VALID/lcr-ac-onlinebrasilv2.crl>

f) “**Authority Information Access**”, **não crítica**: contém o método de acesso `id-ad-caIssuer`, utilizando o protocolo de acesso HTTP, para a recuperação da cadeia de certificação no seguinte endereço:

<http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil/ac-onlinebrasilv2.p7b>

A segunda entrada pode conter o método de acesso `id-ad-ocsp`, com o respectivo endereço do respondedor OCSP, utilizando o protocolo de acesso HTTP, no seguinte

endereço: <http://ocsp.validcertificadora.com.br/ac-onlinebrasil/> Esta extensão somente é aplicável para certificado de usuário final.

g) “*basicConstraints*”, não crítica: contém o campo *cA=False*.

7.1.2.3. Subject Alternative Name

A AC ONLINE BRASIL implementa nos certificados emitidos segundo esta PC a extensão “Subject Alternative Name”, definida pela ICP-Brasil como obrigatória, não crítica, com os seguintes formatos:

a) Para Certificados 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 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

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.

a.2) Não Aplicável

b) Para Certificados 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 *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 Registro Geral (RG) do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva unidade da federação.

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 = nas 14 (quatorze) posições o número do 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.

c) Para Certificados de Equipamento e 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 = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado.

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 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

7.1.2.4. Os campos otherName definidos como obrigatórios pela ICP-Brasil devem estar de acordo com as seguintes especificações:

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

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

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

d) Quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente. No caso de múltiplas habilitações profissionais, deverão ser inseridos e preenchidos os campos (OID) correspondentes às identidades profissionais apresentadas;

e) Todas as informações de tamanho variável referentes a números tais como RG, devem ser preenchidas com caracteres "zero" a sua esquerda para que seja completado seu máximo tamanho possível;

f) As 10 (dez) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF do Título de Eleitor;

g) Apenas os caracteres de A a Z e de 0 a 9 poderão ser utilizados, não sendo permitidos caracteres especiais, símbolos, espaços ou quaisquer outros, com exceção do campo UPN, que utiliza caracteres especiais.

7.1.2.5. Não se Aplica

7.1.2.6. A AC ONLINE BRASIL pode implementar nos certificados emitidos segundo esta PC os seguintes campos, previstos na RFC 5280 e definidos como opcionais pela ICP-Brasil:

a) para Certificados de Pessoa Física

a.1) extensão "Subject Alternative Name":

i. sub-extensão "rfc822Name", contendo o endereço e-mail do titular do certificado.

ii. campo otherName com OID = 1.3.6.1.4.1.311.20.2.3 e conteúdo UPN (User Principal Name), com a identificação do endereço de login do titular do certificado no diretório ActiveDirectory (AD) Microsoft. Esse campo é aplicável apenas em certificados utilizados para logon de rede.

a.2) extensão "Extended Key Usage", não crítica, contendo o valor:

i. "client authentication" (id-kp-clientAuth) (OID 1.3.6.1.5.5.7.3.2);

ii. "e-mail protection" (id-kp-emailProtection) (OID 1.3.6.1.5.5.7.3.4);

iii. "smart card logon" (id-ms-kp-smartcard-logon) (OID 1.3.6.1.4.1.311.20.2.2). Esse campo é aplicável apenas em certificados utilizados para logon de rede.

b) para Certificados de Pessoa Jurídica

b.1) extensão "Subject Alternative Name"

i. sub-extensão "rfc822Name", contendo o endereço e-mail da Pessoa Jurídica titular do certificado.

ii. campo otherName com OID = 1.3.6.1.4.1.311.20.2.3 e conteúdo UPN (User Principal Name), com a identificação do endereço de login do titular do certificado no diretório ActiveDirect (AD) Microsoft. Esse campo é aplicável apenas em certificados utilizados para logon de rede.

b.2) extensão "Extended Key Usage", não crítica, contendo o valor:

i. "client authentication" (id-kp-clientAuth) (OID 1.3.6.1.5.5.7.3.2);

ii. "e-mail protection" (id-kp-emailProtection) (OID 1.3.6.1.5.5.7.3.4);

iii. "smart card logon" (id-ms-kp-smartcard-logon) (OID 1.3.6.1.4.1.311.20.2.2). Esse campo é aplicável apenas em certificados utilizados para logon de rede.

c) para Certificados de Equipamento

c.1) extensão "Subject Alternative Name"

i. sub-extensão "rfc822Name", contendo o endereço e-mail do responsável pelo certificado.

ii. campo otherName com OID = 1.3.6.1.4.1.311.25.1 e conteúdo: identificador único de controlador de domínio (GUID). Esse campo é aplicável somente para certificados de controlador de domínio.

iii. identificação DNS do servidor. Esse campo é aplicável somente para certificados de controlador de domínio.

c.2) extensão "Extended Key Usage", não crítica, contendo o valor:

i. Para certificados de Servidor: "server authentication" (id-kp-serverAuth) (OID 1.3.6.1.5.5.7.3.1);

ii. Para certificados de Equipamento e Controlador de Domínio: "server authentication" (id-kp-serverAuth) (OID 1.3.6.1.5.5.7.3.1) e "client authentication" (id-kp-clientAuth) (OID 1.3.6.1.5.5.7.3.2);

d) para Certificados de Aplicação

d.1) extensão "Subject Alternative Name"

i. sub-extensão "rfc822Name", contendo o endereço e-mail do responsável pelo certificado.

d.2) extensão "Extended Key Usage", não crítica, contendo o valor:

- i. para certificados de Aplicação Assinadora: "client authentication" (id-kp-clientAuth) (OID 1.3.6.1.5.5.7.3.2).
- ii. para certificados de OCSP Responder: "OCSPSigning" (id-kp-OCSPSigning) (OID 1.3.6.1.5.5.7.3.9).
- iii. para certificados de E-mail Seguro: "e-mail protection" (id-kp-emailProtection) (OID 1.3.6.1.5.5.7.3.4).
- iv. Para certificados de Aplicação: "client authentication" (id-kp-clientAuth) (OID 1.3.6.1.5.5.7.3.2) e "e-mail protection" (id-kpemailProtection) (OID 1.3.6.1.5.5.7.3.4).

e) para Certificados de Assinatura de Código

e.1) extensão "Subject Alternative Name"

- i. sub-extensão "rfc822Name", contendo o endereço e-mail do responsável pelo certificado.

e.2) extensão "Extended Key Usage", não crítica, contendo o valor:

- i. "code signing" (id_kp_codeSigning) (OID 1.3.6.1.5.5.7.3.3).

7.1.3. Identificadores de algoritmo

Os certificados emitidos pela AC ONLINE BRASIL são assinados com o uso do algoritmo RSA com SHA-256 como função de hash (OID = 1.2.840.113549.1.1.11), conforme o padrão PKCS#10.

7.1.4 Formatos de Nomes

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 = empresa associada ao emissor do certificado, intermediando o fornecimento de certificados;

OU = nome fantasia (nome que associa uma entidade ao certificado);

OU = unidade (identifica grupo, área, divisão, seção ou qualquer outra identificação semelhante);

OU = referência (indica parâmetro adicional, que pode ser um nome, número, combinação de nome e número ou sequência alfanumérica);

OU = código (número, nome ou sequência alfanumérica);

OU = identificador (sequência alfanumérica);

OU = escopo (finalidade do certificado ou seu domínio de aplicação no contexto de um uso específico);

CN = nome do titular do certificado em certificado de pessoa física; em um certificado de pessoa jurídica, contém o nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica); em um certificado de equipamento ou aplicação, o identificador CN contém o URL correspondente. No caso do certificado de pessoa jurídica para o sistema COMPE, o formato será CCCC-XXX, onde CCCC=quatro posições numéricas contendo o código da instituição financeira e XXX=Nome da Instituição Financeira.

NOTA1: Será escrito o nome até o limite do tamanho do campo disponível, vedada à abreviatura.

NOTA2: Caso qualquer um dos campos OU acima não seja utilizado, o mesmo será grafado com o texto "(EM BRANCO)".

7.1.5. Restrições de nome

7.1.5.1. Não se aplica.

7.1.5.2. A ICP-Brasil estabelece as seguintes restrições para os nomes, aplicáveis a todos os certificados:

- a) não deverão ser utilizados sinais de acentuação, tremas ou cedilhas; e
- b) 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
*	2 ^a
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

7.1.6 OID (Object Identifier) de Política de Certificado

O OID atribuído a esta Política de Certificado é: 2.16.76.1.2.3.45

7.1.7 Uso da extensão “Policy Constraints”

Item não aplicável.

7.1.8 Sintaxe e semântica dos qualificadores de política

Nos certificados emitidos segundo esta PC, o campo **policyQualifiers** da extensão “*Certificate Policies*” contém o endereço da página *Web* (URL) com a DPC da AC ONLINE BRASIL.

<http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil/dpc-ac-onlinebrasil.pdf>

7.1.9. Semântica de processamento para extensões críticas

Extensões críticas são interpretadas conforme a RFC 5280.

7.2. PERFIL DE LCR

7.2.1. Número de versão

As LCRs geradas pela AC ONLINE BRASIL segundo a PC, implementam a versão 2 de LCR definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2 Extensões de LCR e de suas entradas

7.2.2.1 A AC ONLINE BRASIL adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

- a) “*Authority Key Identifier*”, **não crítica**: contém o resumo SHA-1 da chave pública da AC ONLINE BRASIL que assina a LCR; e
- b) “*CRL Number*”, **não crítica**: contém número sequencial para cada LCR emitida.
- c) “*Authority Information Access*”, **não crítica**: contém o método de acesso id-ad-caIssuer, utilizando o protocolo de acesso HTTP, para a recuperação da cadeia de certificação no seguinte endereço:

<http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil/ac-onlinebrasilv2.p7b>

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

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

8.1. PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO

As alterações nas especificações desta PC são realizadas pela AC ONLINE BRASIL. Quaisquer modificações são submetidas à aprovação da AC VALID que as submeterá ao CG da ICP-Brasil.

8.2. POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO

A cada nova versão, esta PC é publicada na página *Web* da AC ONLINE BRASIL www.onlinecertificadora.com.br.

8.3 PROCEDIMENTOS DE APROVAÇÃO

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

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