



***Política de Certificado A1 da
Autoridade Certificadora VALID PLUS SSL
(PC A1 da AC VALID PLUS SSL)***

***OID: 2.16.76.1.2.1.205.
Versão 2.0 de 10/10/2019.***

Conteúdo

1. INTRODUÇÃO	12
1.1. Visão Geral	12
1.2. Nome do Documento e Identificação	13
1.3. PARTICIPANTES DA ICP-BRASIL.....	14
1.3.1. Autoridades Certificadoras.....	14
1.3.2. Autoridades de Registro	14
1.3.3 TITULARES DE CERTIFICADO	15
1.3.4. PARTES CONFIÁVEIS.....	15
1.3.5. OUTROS PARTICIPANTES	15
1.4. USABILIDADE DO CERTIFICADO	15
1.4.1 Uso Adequado do Certificado	15
1.4.2. Uso Proibitivo do Certificado.....	16
1.5. Política de Administração	16
1.5.1. Organização administrativa do documento	16
1.5.2. Contatos.....	16
1.5.3. Pessoa que determina a adequabilidade da DPC com a PC.....	16
1.5. Política de Administração	16
1.5. Definição e Acrônimos	16
2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO.....	18
2.1. Repositórios	18
2.2. Publicação de informações dos certificados	18
2.3. Tempo ou Frequência de Publicação.....	18
2.4. Controle de Acesso aos Repositórios	18
3. IDENTIFICAÇÃO E AUTENTICAÇÃO	18
3.1. Nomeação.....	18
3.1.1. Tipos de nomes	18
3.1.2. Necessidade de nomes significativos	18
3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado	18
3.1.4. Regras para interpretação de vários tipos de nomes.....	18
3.1.5. Unicidade de nomes	18
3.1.6. Procedimento para resolver disputa de nomes.....	18

3.1.7. Reconhecimento, autenticação e papel de marcas registradas.....	18
3.2. Validação Inicial de Identidade	18
3.2.1. Método para comprovar a posse de chave privada	18
3.2.2. Autenticação da identificação da organização	18
3.2.3. Autenticação da identidade de equipamento ou aplicação	18
3.2.4. Autenticação da identidade de um indivíduo	18
3.2.5. Informações não verificadas do titular do certificado	18
3.2.6. Validação das autoridades.....	18
3.2.7. Critérios para interoperação	18
3.3. Identificação e autenticação para pedidos de novas chaves	19
3.3.1. Identificação e autenticação para rotina de novas chaves.....	19
3.3.2. Identificação e autenticação para novas chaves após a revogação	19
3.4. Identificação e Autenticação para solicitação de revogação	19
4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO ..	19
4.1. Solicitação do certificado	19
4.1.1. Quem pode submeter uma solicitação de certificado	19
4.1.2. Processo de registro e responsabilidades	19
4.2. Processamento de Solicitação de Certificado	19
4.2.1. Execução das funções de identificação e autenticação.....	19
4.2.2. Aprovação ou rejeição de pedidos de certificado	19
4.2.3. Tempo para processar a solicitação de certificado	19
4.3. Emissão de Certificado	19
4.3.1. Ações da AC durante a emissão de um certificado	19
4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado	19
4.4. Aceitação de Certificado	19
4.4.1. Conduta sobre a aceitação do certificado	19
4.4.2. Publicação do certificado pela AC	19
4.4.3. Notificação de emissão do certificado pela AC Raiz para outras entidades	19
4.5. Usabilidade do par de chaves e do certificado.....	19
4.5.1. Usabilidade da Chave privada e do certificado do titular	19
4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis	19

4.6. Renovação de Certificados	20
4.6.1. Circunstâncias para renovação de certificados	20
4.6.2. Quem pode solicitar a renovação	20
4.6.3. Processamento de requisição para renovação de certificados	20
4.6.4. Notificação para nova emissão de certificado para o titular	20
4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado	20
4.6.6. Publicação de uma renovação de um certificado pela AC	20
4.6.7. Notificação de emissão de certificado pela AC para outras entidades	20
4.7. Nova chave de certificado.....	20
4.7.1. Circunstâncias para nova chave de certificado.....	20
4.7.2. Quem pode requisitar a certificação de uma nova chave pública	20
4.7.3. Processamento de requisição de novas chaves de certificado.....	20
4.7.4. Notificação de emissão de novo certificado para o titular	20
4.7.5. Conduta constituindo a aceitação de uma nova chave certificada ..	20
4.7.6. Publicação de uma nova chave certificada pela AC	20
4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades	20
4.8. Modificação de certificado	20
4.8.1. Circunstâncias para modificação de certificado	20
4.8.2. Quem pode requisitar a modificação de certificado	20
4.8.3. Processamento de requisição de modificação de certificado	20
4.8.4. Notificação de emissão de novo certificado para o titular	20
4.8.5. Conduta constituindo a aceitação de uma modificação de certificado	20
4.8.6. Publicação de uma modificação de certificado pela AC	20
4.8.7. Notificação de uma emissão de certificado pela AC para outras entidades	20
4.9. Suspensão e Revogação de Certificado	21
4.9.1. Circunstâncias para revogação.....	21
4.9.2. Quem pode solicitar revogação	21
4.9.3. Procedimento para solicitação de revogação	21
4.9.4. Prazo para solicitação de revogação	21

4.9.5. Tempo em que a AC deve processar o pedido de revogação	21
4.9.6. Requisitos de verificação de revogação para as partes confiáveis..	21
4.9.7. Frequência de emissão de LCR	21
4.9.8. Latência máxima para a LCR	21
4.9.9. Disponibilidade para revogação/verificação de status on-line	21
4.9.10. Requisitos para verificação de revogação on-line.....	21
4.9.11. Outras formas disponíveis para divulgação de revogação	21
4.9.12. Requisitos especiais para o caso de comprometimento de chave	21
4.9.13. Circunstâncias para suspensão	21
4.9.14. Quem pode solicitar suspensão.....	21
4.9.15. Procedimento para solicitação de suspensão.....	21
4.9.16. Limites no período de suspensão	21
4.10. Suspensão e Revogação de Certificado	21
4.10.1. Características operacionais.....	21
4.10.2. Disponibilidade dos serviços.....	21
4.10.3. Funcionalidades operacionais	21
4.11. Encerramento de atividades	21
4.12. Custódia e recuperação de chave	21
4.12.1. Política e práticas de custódia e recuperação de chave	21
4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão	22
5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES	22
5.1. Controles físicos.....	22
5.1.1. Construção e localização das instalações	22
5.1.2. Acesso físico.....	22
5.1.3. Energia e ar condicionado	22
5.1.4. Exposição à água	22
5.1.5. Prevenção e proteção contra incêndio.....	22
5.1.6. Armazenamento de mídia	22
5.1.7. Destruição de lixo	22
5.1.8. Instalações de segurança (backup) externas (off-site) para AC	22
5.2. Controles Procedimentais	22

5.2.1. Perfis qualificados.....	22
5.2.2. Número de pessoas necessário por tarefa	22
5.2.3. Identificação e autenticação para cada perfil.....	22
5.2.4. Funções que requerem separação de deveres	22
5.3. Controles de Pessoal	22
5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade.....	22
5.3.2. Procedimentos de verificação de antecedentes	22
5.3.3. Requisitos de treinamento	22
5.3.4. Frequência e requisitos para reciclagem técnica.....	22
5.3.5. Frequência e sequência de rodízio de cargos	22
5.3.6. Sanções para ações não autorizadas.....	22
5.3.7. Requisitos para contratação de pessoal.....	23
5.3.8. Documentação fornecida ao pessoal.....	23
5.4. Procedimentos de Log de Auditoria	23
5.4.1. Tipos de eventos registrados.....	23
5.4.2. Frequência de auditoria de registros.....	23
5.4.3. Período de retenção para registros de auditoria.....	23
5.4.4. Proteção de registros de auditoria	23
5.4.5. Procedimentos para cópia de segurança (Backup) de registros de auditoria.....	23
5.4.6. Sistema de coleta de dados de auditoria (interno ou externo).....	23
5.4.7. Notificação de agentes causadores de eventos	23
5.4.1. Avaliações de vulnerabilidade	23
5.5. Arquivamento de Registros.....	23
5.5.1. Tipos de registros arquivados.....	23
5.5.2. Período de retenção para arquivo.....	23
5.5.3. Proteção de arquivo.....	23
5.5.4. Procedimentos de cópia de arquivo.....	23
5.5.5. Requisitos para datação de registros.....	23
5.5.6. Sistema de coleta de dados de arquivo (interno e externo).....	23
5.5.7. Procedimentos para obter e verificar informação de arquivo	23
5.6. Troca de chave	23
5.7. Comprometimento e Recuperação de Desastre	23

5.7.1. Procedimentos de gerenciamento de incidente e comprometimento	23
5.7.2. Recursos computacionais, software, e/ou dados corrompidos	23
5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade	23
5.5.4. Capacidade de continuidade de negócio após desastre	24
5.8. Extinção da AC	24
6. CONTROLES TÉCNICOS DE SEGURANÇA	24
6.1. Geração e Instalação do par de chaves	24
6.1.1. Geração do par de chaves	24
6.1.2. Entrega da chave privada à entidade	26
6.1.3. Entrega da chave pública para o emissor de certificado	26
6.1.4. Disponibilização de chave pública da AC para usuários	26
6.1.5. Tamanhos de chave	26
6.1.6 Geração de parâmetros de chaves assimétricas	27
6.1.7 Propósitos de uso de chave (conforme o campo “key usage” na X.509 v3)	27
6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico	27
6.2.1. Padrões para módulo criptográfico	27
6.2.2. Controle “n de m” para chave privada	28
Não se aplica	28
6.2.3. Custódia (<i>escrow</i>) de chave privada	28
6.2.4. Cópia de segurança (<i>backup</i>) de chave privada	28
6.2.5 Arquivamento de chave privada	28
6.2.6 Inserção de chave privada em módulo criptográfico	28
Não se aplica	28
6.2.7. Armazenamento de chave privada em módulo criptográfico	28
6.2.8. Método de ativação de chave privada	28
6.2.9. Método de desativação de chave privada	29
6.2.10. Método de destruição de chave privada	29
6.3 Outros Aspectos do Gerenciamento do par de chaves	29
6.3.1 Arquivamento de chave pública	29
6.3.2 Períodos de uso para as chaves pública e privada	29

6.3.2.2 Não se aplica.....	29
6.4 Dados de Ativação.....	29
6.4.1 Geração e instalação dos dados de ativação.....	30
6.4.2 Proteção dos dados de ativação.....	30
6.4.3 Outros aspectos dos dados de ativação.....	30
Não se aplica.....	30
6.5 Controles de Segurança Computacional.....	30
6.5.1 Requisitos técnicos específicos de segurança computacional.....	30
6.5.2 Classificação da segurança computacional.....	30
6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA.....	30
6.6.1. Controles de desenvolvimento de sistema.....	30
6.6.2 Controles de gerenciamento de segurança.....	31
6.6.3 Classificações de segurança de ciclo de vida.....	31
6.6.4 Controles na geração da LCR antes de publicadas.....	31
6.7. Controles de Segurança de Rede.....	31
6.8 Carimbo de Tempo.....	31
7. PERFIS DE CERTIFICADO E LCR E OCSP.....	31
7.1 Perfil do Certificado.....	31
7.1.1 Número de versão.....	32
7.1.2 Extensões de certificado.....	32
7.1.3. Identificadores de algoritmo.....	37
7.1.4 Formatos de nome.....	37
7.1.5. Restrições de nome.....	38
7.1.6 OID (Object Identifier) de Política de Certificado.....	40
7.1.7 Uso da extensão “ <i>Policy Constraints</i> ”.....	40
7.1.8 Sintaxe e semântica dos qualificadores de política.....	40
7.1.9. Semântica de processamento para extensões críticas.....	40
7.2. Perfil de LCR.....	40
7.2.1. Número de versão.....	40
7.2.2 Extensões de LCR e de suas entradas.....	40
7.3. Perfil de OCSP.....	41
7.3.1. Número(s) de versão.....	41
7.3.2. Extensões de OCSP.....	41

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES.....	41
8.1. Frequência e circunstâncias das avaliações.....	41
8.2. Identificação/Qualificação do avaliador.....	41
8.3. Relação do avaliador com a entidade avaliada.....	41
8.4. Tópicos cobertos pela avaliação.....	41
8.5. Ações tomadas como resultado de uma deficiência.....	41
8.6. Comunicação dos resultados.....	41
9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS	41
9.1. Tarifas.....	42
9.1.1. Tarifas de emissão e renovação de certificados.....	42
9.1.2. Tarifas de acesso ao certificado.....	42
9.1.3. Tarifas de revogação ou de acesso à informação de status.....	42
9.1.4. Tarifas para outros serviços.....	42
9.1.5. Política de reembolso.....	42
9.2. Responsabilidade Financeira.....	42
9.2.1. Cobertura do seguro.....	42
9.2.2. Outros ativos.....	42
9.2.3. Cobertura de seguros ou garantia para entidades finais.....	42
9.3. Confidencialidade da informação do negócio.....	42
9.3.1. Escopo de informações confidenciais.....	42
9.3.2. Informações fora do escopo de informações confidenciais.....	42
9.3.3. Responsabilidade em proteger a informação confidencial.....	42
9.4. Privacidade da informação pessoal.....	42
9.4.1. Plano de privacidade.....	42
9.4.2. Tratamento de informação como privadas.....	42
9.4.3. Informações não consideradas privadas.....	42
9.4.4. Responsabilidade para proteger a informação privadas.....	42
9.4.5. Aviso e consentimento para usar informações privadas.....	42
9.4.6. Divulgação em processo judicial ou administrativo.....	42
9.4.7. Outras circunstâncias de divulgação de informação.....	42
9.5. Direitos de Propriedade Intelectual.....	42
9.6. Declarações e Garantias.....	42
9.6.1. Declarações e Garantias da AC.....	42

9.6.2. Declarações e Garantias da AR.....	43
9.6.3. Declarações e garantias do titular.....	43
9.6.4. Declarações e garantias das terceiras partes.....	43
9.6.5. Representações e garantias de outros participantes.....	43
9.7. Isenção de garantias.....	43
9.8. Limitações de responsabilidades.....	43
9.9. Indenizações.....	43
9.10. Prazo e Rescisão.....	43
9.10.1. Prazo.....	43
9.10.2. Término.....	43
9.10.3. Efeito da rescisão e sobrevivência.....	43
9.11. Avisos individuais e comunicações com os participantes.....	43
9.12. Alterações.....	43
9.12.1. Procedimento para emendas.....	43
9.12.2. Procedimento para emendas.....	43
9.12.3. Procedimento para emendas.....	44
9.13. Solução de conflitos.....	44
9.14. Lei aplicável.....	44
9.15. Conformidade com a Lei aplicável.....	44
9.16. Disposições Diversas.....	44
9.16.1. Acordo completo.....	44
10. DOCUMENTOS REFERENCIADOS.....	44

CONTROLE DE ALTERAÇÕES:

Versão	Data	Resolução que aprova a alteração	Item Alterado	Descrição da Alteração
2.0	18/09/2019	Resolução n. 151	Diversos	Alteração da PC A1

1. INTRODUÇÃO

A ICP-Brasil é uma plataforma criptográfica de confiança. Garante presunção de validade jurídica aos atos e negócios eletrônicos assinados e cifrados com certificados digitais e chaves emitidos pelas entidades credenciadas na ICP-Brasil.

1.1. Visão Geral

1.1.1. Este documento estabelece requisitos mínimos a serem obrigatoriamente observados pelas Autoridades Certificadoras – AC integrantes da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) na elaboração de suas Políticas de Certificado (PC)

1.1.2. Toda PC elaborada no âmbito da ICP-Brasil deve obrigatoriamente adotar a mesma estrutura empregada neste documento.

1.1.3. São 12 (doze) os tipos, inicialmente previstos, de certificados digitais para usuários finais da ICP-Brasil, sendo 8 (oito) relacionados com assinatura digital e 4 (quatro) com sigilo, conforme o descrito a seguir:

a) Tipos de Certificados de Assinatura Digital:

- ✓ A1
- ✓ A2
- ✓ A3
- ✓ A4
- ✓ T3
- ✓ T4
- ✓ A CF-e-SAT
- ✓ OM-BR

b) Tipos de Certificados de Sigilo:

- ✓ S1
- ✓ S2
- ✓ S3
- ✓ S4

1.1.4. Os tipos de certificados indicados acima, de A1 a A4 e de S1 a S4, definem escalas de requisitos de segurança, nas quais os tipos A1 e S1 estão associados aos requisitos menos rigorosos e os tipos A4 e S4 aos requisitos mais rigorosos.

1.1.5. Certificados dos tipos de A1 a A4 e de S1 a S4, de assinatura ou de sigilo, podem, conforme a necessidade, ser emitidos pelas ACs para pessoas físicas, pessoas jurídicas, equipamentos ou aplicações.

1.1.6. Certificados do tipo T3 e T4 somente podem ser emitidos para equipamentos das Autoridades de Carimbo de Tempo (ACTs) credenciadas na ICP-Brasil. Os certificados do tipo T3 e T4 estão associados aos mesmos requisitos de segurança, exceto pelo tamanho das chaves criptográficas utilizadas.

1.1.7. Certificados do tipo A CF-e-SAT só podem ser emitidos para equipamentos integrantes do Sistema de Autenticação e Transmissão do Cupom Fiscal Eletrônico – SAT-CF-e, seguindo a regulamentação do CONFAZ.

1.1.8. Certificados do tipo Objeto Metrológico – OM-BR só podem ser emitidos para equipamentos metrológicos regulados pelo Inmetro.

1.1.9. Outros tipos de certificado, além dos doze anteriormente relacionados, podem ser propostos para a apreciação do Comitê Gestor da ICP-Brasil – CG da ICP-Brasil. As propostas serão analisadas quanto à conformidade com as normas específicas da ICP-Brasil e, quando aprovadas, serão acrescentadas aos tipos de certificados aceitos pela ICP-Brasil.

1.1.10. Para certificados com propósito de uso EV SSL e EV CS devem ser observados os dispostos nos documentos EV SSL/CS Guidelines.

1.2. Nome do Documento e Identificação

1.2.1. Esta PC é chamada “Política de Certificado de Equipamento Servidor Tipo A1 da Autoridade Certificadora VALID PLUS SSL” e referida como “PC A1 da AC VALID PLUS SSL”. O Object Identifier (OID) atribuído para esta PC, após processo de credenciamento da AC junto à ICP-Brasil, é: **2.16.76.1.2.1.205**.

1.2.2. No âmbito da ICP-Brasil, os OIDs das PCs serão atribuídos na conclusão do processo de credenciamento da AC, conforme a Tabela 3 a seguir:

Tabela 1 - OID de PC na ICP-Brasil

Tipo de Certificado	OID
A1	2.16.76.1.2.1.n
A2	2.16.76.1.2.2.n
A3	2.16.76.1.2.3.n
A4	2.16.76.1.2.4.n
S1	2.16.76.1.2.101.n
S2	2.16.76.1.2.102.n
S3	2.16.76.1.2.103.n
S4	2.16.76.1.2.104.n
T3	2.16.76.1.2.303.n
T4	2.16.76.1.2.304.n
A CF-e-SAT	2.16.76.1.2.500.n
OM-BR	2.16.76.1.2.550.n

1.3. PARTICIPANTES DA ICP-BRASIL

1.3.1. Autoridades Certificadoras

1.3.1.1. Esta PC é implementada pela Autoridade Certificadora AC VALID PLUS SSL, integrante da Infraestrutura de Chaves Públicas Brasileira, ICP-Brasil, sob a hierarquia da Autoridade Certificadora BRASIL, 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 VALID PLUS SSL estão descritas em sua Declaração de Práticas de Certificação (DPC da AC VALID PLUS SSL) que se encontra publicada no seu repositório, no seguinte endereço: <http://www.validcertificadora.com.br/>

1.3.2. Autoridades de Registro

1.3.2.1. A AC VALID PLUS SSL mantém página web e/ou diretório com endereço: <http://www.validcertificadora.com.br/> 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;
- b) Relação de AR que tenham se descredenciado da cadeia da AC VALID PLUS SSL, com respectiva data do descredenciamento.

1.3.2.2. A AC VALID PLUS SSL mantém as informações acima sempre atualizadas.

1.3.3 TITULARES DE CERTIFICADO

Os titulares dos certificados emitidos nesta PC são pessoas jurídicas de direito público ou privado, nacionais ou estrangeiras.

1.3.4. PARTES CONFIÁVEIS

Considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do certificado digital e chaves emitidas pela ICP-Brasil

1.3.5. OUTROS PARTICIPANTES

1.3.5.1. A relação de todos os Prestadores de Serviços de Suporte – PSS, Prestadores de Serviços Biométricos – PSBios e Prestadores de Serviço de Confiança – PSC vinculados à AC VALID PLUS SSL e/ou por intermédio de suas AR é publicada em serviço de diretório e/ou em página web da AC VALID PLUS SSL (<http://www.validcertificadora.com.br/>).

1.4. USABILIDADE DO CERTIFICADO

1.4.1 Uso Adequado do Certificado

1.4.1.1. Neste item são relacionadas as aplicações para as quais os certificados definidos nesta PC são adequados.

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

1.4.1.3. A AC VALID PLUS SSL 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.

Os certificados emitidos pela AC VALID PLUS SSL 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.

1.4.1.4. Certificados de tipos A1 e A3 serão utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.4.2. Uso Proibitivo do Certificado

Não se aplica.

1.5. Política de Administração

1.5.1. Organização administrativa do documento

Nome da AC: VALID CERTIFICADORA DIGITAL LTDA.

1.5.2. Contatos

Endereço: Avenida Paulista, nº 2064, 15º andar, Bela Vista São Paulo, SP -

CEP: 01310-928

Telefone: (11)2575-6800

Página Web: <http://www.validcertificadora.com.br>

E-mail: pki.compliance@valid.com

1.5.3. Pessoa que determina a adequabilidade da DPC com a PC

Nome: Márcio Nunes da Silva

E-mail: pki.compliance@valid.com

Telefones: (11)2575-6800

1.5. Política de Administração

Esta PC é aprovada pelo ITI. Os procedimentos de aprovação da PC da AC são estabelecidos a critério do CG da ICP-Brasil.

1.5. Definição e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	<i>Capability Maturity Model do Software Engineering Institute</i>
CMVP	<i>Cryptographic Module Validation Program</i>
CN	<i>Common Name</i>
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COBIT	<i>Control Objectives for Information and related Technology</i>

COSO	<i>Comitee of Sponsoring Organizations</i>
CONFAZ	Conselho Nacional de Política Fazendária
CPF	Cadastro de Pessoas Físicas
CS	<i>Code Signing</i>
DMZ	Zona Desmilitarizada
DN	<i>Distinguished Name</i>
DPC	Declaração de Práticas de Certificação
EV	<i>Extended Validation</i>
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	<i>Intrusion Detection System</i>
IEC	<i>International Electrotechnical Commission</i>
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	<i>International Organization for Standardization</i>
ITSEC	<i>European Information Technology Security Evaluation Criteria</i>
ITU	<i>International Telecommunications Union</i>
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIST	<i>National Institute of Standards and Technology</i>
NIS	Número de Identificação Social
OCSP	<i>Online Certificate Status Protocol</i>
OID	<i>Object Identifier</i>
OM-BR	Objetos Metrológicos ICP-Brasil
OU	<i>Organization Unit</i>
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	<i>Proof of Possession</i>
PS	Política de Segurança
PSS	Prestadores de Serviço de Suporte
RFC	<i>Request For Comments</i>
RG	Registro Geral
SAT	Sistema de Autenticação e Transmissão
SNMP	<i>Simple Network Management Protocol</i>
SSL	<i>Secure Socket Layer</i>
TCSEC	<i>Trusted System Evaluation Criteria</i>
TSDM	<i>Trusted Software Development Methodology</i>
UF	Unidade de Federação
URL	<i>Uniform Resource Locator</i>

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

Nos itens seguintes são referidos os itens correspondentes da Declaração de Práticas de Certificação - DPC da AC VALID PLUS SSL.

2.1. Repositórios

2.2. Publicação de informações dos certificados

2.3. Tempo ou Frequência de Publicação

2.4. Controle de Acesso aos Repositórios

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

Nos itens seguintes são referidos os itens correspondentes da Declaração de Práticas de Certificação - DPC da AC VALID PLUS SSL.

3.1. Nomeação

3.1.1. Tipos de nomes

3.1.2. Necessidade de nomes significativos

3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado

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

3.2. Validação Inicial de Identidade

3.2.1. Método para comprovar a posse de chave privada

3.2.2. Autenticação da identificação da organização

3.2.3. Autenticação da identidade de equipamento ou aplicação

3.2.4. Autenticação da identidade de um indivíduo

3.2.5. Informações não verificadas do titular do certificado

3.2.6. Validação das autoridades

3.2.7. Critérios para interoperação

3.3. Identificação e autenticação para pedidos de novas chaves

3.3.1. Identificação e autenticação para rotina de novas chaves

3.3.2. Identificação e autenticação para novas chaves após a revogação

3.4. Identificação e Autenticação para solicitação de revogação

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

Nos itens seguintes são referidos os itens correspondentes da Declaração de Práticas de Certificação - DPC da AC VALID PLUS SSL.

4.1. Solicitação do certificado

4.1.1. Quem pode submeter uma solicitação de certificado

4.1.2. Processo de registro e responsabilidades

4.2. Processamento de Solicitação de Certificado

4.2.1. Execução das funções de identificação e autenticação

4.2.2. Aprovação ou rejeição de pedidos de certificado

4.2.3. Tempo para processar a solicitação de certificado

4.3. Emissão de Certificado

4.3.1. Ações da AC durante a emissão de um certificado

4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado

4.4. Aceitação de Certificado

4.4.1. Conduta sobre a aceitação do certificado

4.4.2. Publicação do certificado pela AC

4.4.3. Notificação de emissão do certificado pela AC Raiz para outras entidades

4.5. Usabilidade do par de chaves e do certificado

4.5.1. Usabilidade da Chave privada e do certificado do titular

4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis

4.6. Renovação de Certificados

4.6.1. Circunstâncias para renovação de certificados

4.6.2. Quem pode solicitar a renovação

4.6.3. Processamento de requisição para renovação de certificados

4.6.4. Notificação para nova emissão de certificado para o titular

4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado

4.6.6. Publicação de uma renovação de um certificado pela AC

4.6.7. Notificação de emissão de certificado pela AC para outras entidades

4.7. Nova chave de certificado

4.7.1. Circunstâncias para nova chave de certificado

4.7.2. Quem pode requisitar a certificação de uma nova chave pública

4.7.3. Processamento de requisição de novas chaves de certificado

4.7.4. Notificação de emissão de novo certificado para o titular

4.7.5. Conduta constituindo a aceitação de uma nova chave certificada

4.7.6. Publicação de uma nova chave certificada pela AC

4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades

4.8. Modificação de certificado

4.8.1. Circunstâncias para modificação de certificado

4.8.2. Quem pode requisitar a modificação de certificado

4.8.3. Processamento de requisição de modificação de certificado

4.8.4. Notificação de emissão de novo certificado para o titular

4.8.5. Conduta constituindo a aceitação de uma modificação de certificado

4.8.6. Publicação de uma modificação de certificado pela AC

4.8.7. Notificação de uma emissão de certificado pela AC para outras entidades

entidades

4.9. Suspensão e Revogação de Certificado

4.9.1. Circunstâncias para revogação

4.9.2. Quem pode solicitar revogação

4.9.3. Procedimento para solicitação de revogação

4.9.4. Prazo para solicitação de revogação

4.9.5. Tempo em que a AC deve processar o pedido de revogação

4.9.6. Requisitos de verificação de revogação para as partes confiáveis

4.9.7. Frequência de emissão de LCR

4.9.8. Latência máxima para a LCR

4.9.9. Disponibilidade para revogação/verificação de status on-line

4.9.10. Requisitos para verificação de revogação on-line

4.9.11. Outras formas disponíveis para divulgação de revogação

4.9.12. Requisitos especiais para o caso de comprometimento de chave

4.9.13. Circunstâncias para suspensão

4.9.14. Quem pode solicitar suspensão

4.9.15. Procedimento para solicitação de suspensão

4.9.16. Limites no período de suspensão

4.10. Suspensão e Revogação de Certificado

4.10.1. Características operacionais

4.10.2. Disponibilidade dos serviços

4.10.3. Funcionalidades operacionais

4.11. Encerramento de atividades

4.12. Custódia e recuperação de chave

4.12.1. Política e práticas de custódia e recuperação de chave

4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Nos itens seguintes são referidos os itens correspondentes da Declaração de Práticas de Certificação - DPC da AC VALID PLUS SSL.

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) para AC

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

5.2.4. Funções que requerem separação de deveres

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

5.4. Procedimentos de Log de Auditoria

5.4.1. Tipos de eventos registrados

5.4.2. Frequência de auditoria de registros

5.4.3. Período de retenção para registros de auditoria

5.4.4. Proteção de registros de auditoria

5.4.5. Procedimentos para cópia de segurança (Backup) de registros de auditoria

5.4.6. Sistema de coleta de dados de auditoria (interno ou externo)

5.4.7. Notificação de agentes causadores de eventos

5.4.1. Avaliações de vulnerabilidade

5.5. Arquivamento de Registros

5.5.1. Tipos de registros arquivados

5.5.2. Período de retenção para arquivo

5.5.3. Proteção de arquivo

5.5.4. Procedimentos de cópia de arquivo

5.5.5. Requisitos para datação de registros

5.5.6. Sistema de coleta de dados de arquivo (interno e externo)

5.5.7. Procedimentos para obter e verificar informação de arquivo

5.6. Troca de chave

5.7. Comprometimento e Recuperação de Desastre

5.7.1. Procedimentos de gerenciamento de incidente e comprometimento

5.7.2. Recursos computacionais, software, e/ou dados corrompidos

5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade

5.5.4. Capacidade de continuidade de negócio após desastre

5.8. Extinção da AC

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, esta PC define as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo a mesma. São também definidos outros controles técnicos de segurança utilizados pela AC VALID PLUS SSL 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. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(is), a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.

6.1.1.1.1. Não se aplica.

6.1.1.1.2. Não se aplica

6.1.1.2. A geração do par de chaves criptográficas ocorre, no mínimo, utilizando CSP (Cryptographic Service Provider) existente na estação do solicitante apresentados pelo browser 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 – hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO - 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 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. 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 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. Esta mídia de armazenamento não deve modificar os dados a serem assinados, nem impedir que esses dados sejam apresentados ao signatário antes do processo de assinatura.

6.1.1.8. O armazenamento de chaves privadas de terceiros em hardware criptográfico só poderá ser realizada por entidade credenciada como PSC, nos termos do DOC-ICP-17[4], ou no caso de soluções corporativas de armazenamento de chaves privadas de funcionários, em HSM de propriedade da instituição, mediante o conhecimento e concordância expressa do titular do certificado com a DPC da AC VALID PLUS SSL, que atendam as aplicações demandadas das organizações, com acesso exclusivo por meio da rede interna.

O tipo de certificado emitido pela AC VALID PLUS SSL e descrito nesta PC é o A1.

TIPO DE CERTIFICADO	MÍDIA ARMAZENADORA DE CHAVE CRIPTOGRÁFICA (Requisitos Mínimos)
A1	Repositório protegido por senha e/ou identificação biométrica, cifrado por <i>software</i> na forma definida acima.

Nota: A responsabilidade pela segurança na garantia do sigilo, integridade e disponibilidade da chave privada gerada no equipamento é do titular ou responsável pelo uso do certificado, conforme especificado no Termo de Titularidade.

Nota 2: para certificados do tipo A CF-e-SAT, T3 e T4, a exigência de homologação ou certificação das mídias para geração e armazenamento de chaves criptográficas fica suspensa até ulterior deliberação do Comitê Gestor da ICP-Brasil.

6.1.2. Entrega da chave privada à entidade

Não se aplica.

6.1.3. Entrega da chave pública para o emissor de certificado

Chaves públicas são entregues à AC VALID PLUS SSL por meio de uma troca *on-line* utilizando funções automáticas do *software* de certificação da AC VALID PLUS SSL. 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.

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

6.1.4. Disponibilização de chave pública da AC para usuários

As formas para a disponibilização dos certificados da cadeia de certificação, para os usuários da AC VALID PLUS SSL, compreendem:

A AC VALID PLUS SSL 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.validcertificadora.com.br/ac-validplussl/ac-validplusslv5.p7b>

(Para cadeia V5)

- a) Página *web* da AC VALID PLUS SSL <http://www.validcertificadora.com.br>
- b) 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 e V5). O tamanho das chaves criptográficas associadas é de 2048 bits.

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

6.1.6 Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas da AC VALID PLUS SSL seguem o padrão FIPS (Federal Information Processing Standards) 140-1, em conformidade ao estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

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

Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

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

Os certificados têm ativados os bits digitalSignature, nonRepudiation e keyEncipherment. Os pares de chaves correspondentes aos certificados emitidos pela AC VALID PLUS SSL podem ser utilizados para a assinatura digital (chave privada), para a verificação dela (chave pública), para a garantia do não repúdio e para cifragem de chaves.

6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico

Nos itens seguintes, a PC define os requisitos para a proteção das chaves privadas dos titulares de certificados emitidos pela AC VALID PLUS SSL.

6.2.1. Padrões para módulo criptográfico

6.2.1.1. Não se aplica

6.2.1.2. Os requisitos aplicáveis ao módulo criptográfico utilizado para geração de chaves criptográficas dos titulares de certificado segue os definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

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-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 VALID PLUS SSL 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. Não se aplica, 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. Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

6.2.8. Método de ativação de chave privada

A chave privada é ativada mediante senha solicitada pelo *software* de proteção da chave privada.

6.2.9. Método de desativação de chave privada

Cada entidade titular de certificado pode definir os procedimentos necessários para a desativação da sua chave privada.

6.2.10. Método de destruição de chave privada

Cada entidade titular de certificado pode definir os procedimentos necessários para a destruição da 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 VALID PLUS SSL, de titulares dos certificados de assinatura digital e as *LCRs* emitidas pela AC VALID PLUS SSL 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 A1 previstos nesta PC podem ter a validade de minutos, horas, dias e até 1 (um) ano.

6.3.2.4. O período máximo de validade dos Certificados de Assinatura de Código será de até 39 (trinta e nove) meses, conforme princípios e critérios Webtrust.

6.3.2.5. O período máximo de validade dos Certificados SSL/TLS será de até 825 (oitocentos e vinte cinco) dias, conforme princípios e critérios Webtrust.

6.4 Dados de Ativação

Nos itens seguintes desta PC são descritos os requisitos de segurança referentes aos dados de ativação. Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos.

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 antivírus e criptografia 3DES 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

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

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

6.6.2 Controles de gerenciamento de segurança

6.6.2.1. A AC VALID PLUS SSL 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 VALID PLUS SSL 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.

6.6.4 Controles na geração da LCR antes de publicadas

Antes de publicadas, todas as LCRs geradas pela AC VALID PLUS SSL são checadas quanto à consistência de seu conteúdo, comparando-o com o conteúdo esperado em relação a número da LCR, data/hora de emissão e outras informações relevantes.

6.7. Controles de Segurança de Rede

Não se aplica.

6.8 Carimbo de Tempo

Em acordo com os REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL[5].

7. PERFIS DE CERTIFICADO E LCR E OCSP

Os itens seguintes especificam os formatos dos certificados e das LCR/ OCSP 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 VALID PLUS SSL estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.1.1 Número de versão

Todos os certificados emitidos pela AC VALID PLUS SSL, 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 pela AC VALID PLUS SSL e sua criticalidade.

7.1.2.2. A AC VALID PLUS SSL 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 VALID PLUS SSL;
- b) "**Key Usage**", **crítica**: somente os bits `digitalSignature`, `nonRepudiation` e `keyEncipherment` são ativados;
- c) "**Certificate Policies**", **não crítica**, contém
 - ✓ O campo `policyIdentifier` contém o OID desta PC **2.16.76.1.2.1.205**.
 - ✓ O campo `PolicyQualifiers` contém o endereço *Web* onde se obtém a DPC da AC VALID PLUS SSL, onde:

Para Certificados Digitais emitidos na cadeia V5:

<http://icp-brasil.validcertificadora.com.br/ac-validplussl/lcr-ac-validplusslv5.crl>

- d) "**CRL Distribution Points**", **não crítica**: contém o endereço *URL* das páginas *Web* onde se obtém a LCR da AC VALID PLUS SSL:

Para Certificados Digitais emitidos na cadeia V5:

1) <http://icp-brasil.validcertificadora.com.br/ac-validplussl/lcr-ac-validplusslv5.crl>

2) <http://icp-brasil2.validcertificadora.com.br/ac-validplussl/lcr-ac-validplusslv5.crl>

- e) "**Authority Information Access**", **não crítica**: contém o método de acesso `id-ad-calssuer`, utilizando o protocolo de acesso HTTP, para a recuperação da cadeia de certificação.

Para certificados digitais emitidos na cadeia V5:

<http://icp-brasil.validcertificadora.com.br/ac-validplussl/ac-validplusslv5.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, nos seguintes endereços, onde estas extensões somente serão aplicáveis para certificados de usuário final:

Para certificados digitais emitidos na cadeia V2:

<http://ocsp.validcertificadora.com.br>

Para certificados digitais emitidos na cadeia V5:

<http://ocspv5.validcertificadora.com.br>

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

7.1.2.3. A ICP-Brasil também define como obrigatória a extensão "Subject Alternative Name", não crítica, e com os seguintes formatos:

a) Para certificado de pessoa física:

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

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

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

iii- OID = 2.16.76.1.3.5 e conteúdo nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subsequentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subsequentes, o município e a UF do Título de Eleitor;

iv. campo rfc822Name contendo o endereço e-mail do titular do certificado

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

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) 5 (cinco) campos otherName, obrigatórios, contendo:

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; Política de Certificado de «PCas_» Tipo «tipo» da «AC_EXTENSO» PC «tipo» da «AC» v «VERSAO» 22/29

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;

v. campo rfc822Name contendo o endereço e-mail do titular do certificado.

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

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, aplicação e OCSP.

Esta PC não implementa a emissão de certificados e-Servidor, e-Aplicação e e-Código

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

i. OID = 2.16.76.1.3.8 e conteúdo = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, se o certificado for de pessoa jurídica;

ii. OID = 2.16.76.1.3.3 e conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ), se o certificado for de pessoa jurídica;

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

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

v. campo rfc822Name contendo o endereço e-mail do titular do certificado.

c.2) Para certificados do tipo SSL/TLS, Campo dNSName, obrigatório, contendo um ou mais domínios pertencentes ou controlados pelo titular, seguindo as regras definidas na RFC 5280 e RFC 2818, em conformidade com os princípios e critérios WebTrust.

d) não se aplica.

e) não se aplica.

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) 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, tal como RG, são 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, sendo 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, de 0 a 9, observado o disposto no item 7.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais, com exceção do campo UPN que utiliza caracteres especiais;

h) 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 VALID PLUS SSL, podem ser utilizados com OID atribuídos ou aprovados pela AC Raiz.

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

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

7.1.2.7. As extensões "*Key Usage*" e "*Extended Key Usage*" para os referidos tipos de certificado são obrigatórias e obedecem os propósitos de uso e a criticidade conforme descrição abaixo:

a) para certificados de Assinatura de Código (`codeSigning`):
"*Key Usage*", crítica: somente o bit `digitalSignature` está ativado;
"*Extended Key Usage*", não crítica: somente o `codeSigning` OID = 1.3.6.1.5.5.7.3.3 está presente;

b) para certificados de Autenticação de Servidor (SSL/TLS):
"*Key Usage*", crítica: somente os bits `digitalSignature`, `keyEncipherment` ou `keyAgreement` estão ativados;
"*Extended Key Usage*", não crítica: contém o propósito `server authentication` OID = 1.3.6.1.5.5.7.3.1. Pode conter o propósito `client authentication` OID = 1.3.6.1.5.5.7.3.2;

c) Para certificados de Assinatura de Carimbo do Tempo:
"*Key Usage*", crítica: somente os bits `digitalSignature` e `nonRepudiation` estão ativados; "*Extended Key Usage*", crítica: somente o propósito `timeStamping` OID = 1.3.6.1.5.5.7.3.8 está presente nos certificados de equipamentos de carimbo do tempo de ACT credenciada na ICP-Brasil. Esse OID não deve ser empregado em qualquer outro tipo de certificado;

- d) Para certificados de Assinatura A CF-e-SAT:
"Key Usage", crítica: contém o bit digitalSignature ativado, podendo conter os bits keyAgreement e nonRepudiation ativados; "Extended Key Usage", não crítica: somente o propósito client authentication OID = 1.3.6.1.5.5.7.3.2 está presente;
- e) Para certificados de Assinatura de Resposta OCSP:
"Key Usage", crítica: contém o bit digitalSignature ativado, podendo conter o bit nonRepudiation ativado; "Extended Key Usage", não crítica: somente o propósito OCSPSigning OID = 1.3.6.1.5.5.7.3.9 está presente;
- f) Para os demais certificados de Assinatura e/ou Proteção de e-Mail:
"Key Usage", crítica: contém o bit digitalSignature ativado, podendo conter os bits keyEncipherment e nonRepudiation ativados;
"Extended Key Usage", não crítica: no mínimo um dos propósitos client authentication OID = 1.3.6.1.5.5.7.3.2 ou E-mail protection OID = 1.3.6.1.5.5.7.3.4 está ativado, podendo implementar outros propósitos instituídos, desde que verificáveis e previstos nesta PC, em conformidade com a RFC 5280; e
- g) Para certificados de Sigilo:
"Key Usage", crítica: somente os bits keyEncipherment e dataEncipherment estão ativados.

7.1.3. Identificadores de algoritmo

Certificados emitidos pela AC VALID PLUS SSL são assinados com o uso do 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 hash (OID = 1.2.840.113549.1.1.13), 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 = AC VALID PLUS SSL

OU = <Identificação da AR>

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

OU = identificador (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);

OU = o CNPJ da AR que realizou a identificação presencial;

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 CCCCXXX, onde CCCC=quatro posições numéricas contendo o código da instituição financeira e XXX=Nome da Instituição Financeira.

Onde:

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 aplicação OCSP, o identificador CN contém o nome da aplicação.

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

O campo OU = indica o <CNPJ da AR> onde ocorreu a identificação presencial, que será preenchido com 14 (quatorze) posições, sem caracteres como ".", "/" ou "-".

O Campo E (endereço e-mail do titular do certificado) deixou de compor o "Distinguished Name" (DN) a partir da implementação da cadeia V5.

7.1.4.2. Não se aplica.

7.1.4.3. Não se aplica.

7.1.4.4. Não se aplica.

7.1.5. Restrições de nome

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

7.1.5.2. 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: **2.16.76.1.2.1.205**.

Todo certificado emitido segundo essa PC, PC A1 AC VALID PLUS SSL, contém o valor desse OID presente na extensão Certificate Policies

7.1.7 Uso da extensão “*Policy Constraints*”

Não se aplica.

7.1.8 Sintaxe e semântica dos qualificadores de política

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 VALID PLUS SSL, sendo:

<http://icp-brasil.validcertificadora.com.br/ac-validplussl/dpc-ac-validplussslv5.pdf>

7.1.9. Semântica de processamento para extensões críticas

Extensões críticas são ser interpretadas conforme a RFC 5280.

7.2. Perfil de LCR

7.2.1. Número de versão

As LCRs geradas pela AC VALID PLUS SSL 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. Neste item são descritas todas as extensões de LCR utilizadas pela AC VALID PLUS SSL e sua criticalidade.

7.2.2.2. A AC VALID PLUS SSL 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 VALID PLUS SSL 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-calssuer*, utilizando o protocolo de acesso HTTP, para a recuperação da cadeia de certificação nos seguintes endereços:

Para Certificados Digitais emitidos na cadeia V5:

<http://icp-brasil.validcertificadora.com.br/ac-validplussssl/ac-validplusssslv5.p7b>

7.3. Perfil de OCSP

7.3.1. Número(s) de versão

Os serviços de respostas OCSP da AC VALID PLUS SSL implementam a versão 1. do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 6960

7.3.2. Extensões de OCSP

Os serviços de respostas OCSP da AC VALID PLUS SSL estão em conformidade com a RFC 6960.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Nos itens seguintes são referidos os itens correspondentes da DPC da AC VALID PLUS SSL.

8.1. Frequência e circunstâncias das avaliações

8.2. Identificação/Qualificação do avaliador

8.3. Relação do avaliador com a entidade avaliada

8.4. Tópicos cobertos pela avaliação

8.5. Ações tomadas como resultado de uma deficiência

8.6. Comunicação dos resultados

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

Nos itens seguintes são referidos os itens correspondentes da DPC da AC VALID PLUS SSL.

9.1. Tarifas

9.1.1. Tarifas de emissão e renovação de certificados

9.1.2. Tarifas de acesso ao certificado

9.1.3. Tarifas de revogação ou de acesso à informação de status

9.1.4. Tarifas para outros serviços

9.1.5. Política de reembolso

9.2. Responsabilidade Financeira

9.2.1. Cobertura do seguro

9.2.2. Outros ativos

9.2.3. Cobertura de seguros ou garantia para entidades finais

9.3. Confidencialidade da informação do negócio

9.3.1. Escopo de informações confidenciais

9.3.2. Informações fora do escopo de informações confidenciais

9.3.3. Responsabilidade em proteger a informação confidencial

9.4. Privacidade da informação pessoal

9.4.1. Plano de privacidade

9.4.2. Tratamento de informação como privadas

9.4.3. Informações não consideradas privadas

9.4.4. Responsabilidade para proteger a informação privadas

9.4.5. Aviso e consentimento para usar informações privadas

9.4.6. Divulgação em processo judicial ou administrativo

9.4.7. Outras circunstâncias de divulgação de informação

9.5. Direitos de Propriedade Intelectual

9.6. Declarações e Garantias

9.6.1. Declarações e Garantias da AC

9.6.2. Declarações e Garantias da AR

9.6.3. Declarações e garantias do titular

9.6.4. Declarações e garantias das terceiras partes

9.6.5. Representações e garantias de outros participantes

9.7. Isenção de garantias

9.8. Limitações de responsabilidades

9.9. Indenizações

9.10. Prazo e Rescisão

9.10.1. Prazo

9.10.2. Término

9.10.3. Efeito da rescisão e sobrevivência

9.11. Avisos individuais e comunicações com os participantes

9.12. Alterações

9.12.1. Procedimento para emendas

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

Qualquer alteração na PC deverá ser submetida à aprovação da AC Raiz.

9.12.2. Procedimento para emendas

A AC VALID PLUS SSL mantém página específica com a versão corrente desta PC para consulta pública, a qual está disponibilizada no endereço Web <http://icp-brasil.validcertificadora.com.br/ac-validplussssl/dpc-ac-validplussssl5.pdf>

9.12.3. Procedimento para emendas**9.13. Solução de conflitos****9.14. Lei aplicável****9.15. Conformidade com a Lei aplicável****9.16. Disposições Diversas****9.16.1. Acordo completo**

Esta PC representa as obrigações e deveres aplicáveis à AC VALID PLUS SSL e AR e outras entidades citadas. Havendo conflito entre esta PC e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

10. 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
[4]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL	DOC-ICP-17
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP-12
[6]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04

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

REF.	NOME DO DOCUMENTO	CÓDIGO
[1]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01
[2]	ATRIBUIÇÃO DE OID NA ICP-BRASIL	DOC-ICP-04.01