Política de Certificado de Assinatura Digital Tipo A3 da Autoridade Certificadora Certisign ICP-Brasil SSL

PC A3 da AC Certisign ICP-Brasil SSL

Versão 2.4 – 03/04/2023

Sumário

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item Alterado	Descrição da Alteração
1.0	29/07/2020	Não se aplica	Vários	Criação da AC Certisign ICP-Brasil SSL
1.1	21/12/2020	Não se aplica	7.1.2.1, 7.1.8	Correção do endereço de repositório da DPC
2.0	18/06/2021	Resolução 179	1 ao 1.1.12	Adequação a resolução
			1.6	Atualização de acrônimos
			11	Atualização das referências bibliográficas
		Não se aplica	7.1.2.3 c.1)	Deixar o item como Não se aplica.
2.1	01/07/2021	Não se aplica	7.1.2.7	Criação do item b.1) para o Open Banking
			7.1.4.4.1	Criação do item para o Open Banking
2.2	08/09/2021	Não se aplica	7.1.2.1 d) e e)	Inclusão da url G2.
2.3	16/12/2022	Não se aplica	7.1.2.1 d) e e)	Inclusão da url G3
			7.1.2.7 b.2)	Inclusão do item
			7.1.4.4.1	Alteração de texto
			7.1.4.4.2 e 7.1.4.4.3	Inclusão do item
2.4	03/04/2023	Não se aplica	6.1.4, 7.1.2.1 d) e e)	Inclusão da url G4

Política de Certificado de Assinatura Digital Tipo A3 da Autoridade Certificadora Certisign ICP-Brasil SSL

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Esta "Política de Certificado" (PC) descreve as políticas de certificação de certificados de Assinatura Digital Tipo A3 da Autoridade Certificadora Certisign ICP-BRASIL SSL na Infraestrutura de Chaves Públicas Brasileira.

1.1.2 A estrutura desta PC está baseada no DOC-ICP-04 – REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL[6].

1.1.3 A estrutura desta PC está baseada na RFC 3647.

1.1.4 Este documento compõe o conjunto da ICP-Brasil e nele são referenciados outros regulamentos dispostos nas demais normas da ICP-Brasil, conforme especificado no item 10

1.1.5 Essa PC se refere ao Certificado de Assinatura Digital Tipo A3.

1.1.6 Não se aplica.

1.1.7 Não se aplica.

1.1.8 Não se aplica.

1.1.9 Não se aplica.

1.1.10 Não se aplica.

1.1.11 Não se aplica.

1.1.12 Para certificados com propósito de uso EV SSL são observados os dispostos nos documentos EV SSL Guidelines.

1.2. Nome do documento e identificação

1.2.1. Esta PC é chamada "Política de Certificado de assinatura digital Tipo A3 da Autoridade Certificadora Certisign ICP-BRASIL SSL" e referida como "PC A3 da AC Certisign ICP-Brasil SSL". Esta PC descreve os usos relacionados ao certificado de assinatura digital correspondente ao tipo A3 no DOC-ICP-04 do Comitê Gestor da ICP-Brasil. O OID (object identifier) desta PC é 2.16.76.1.2.3.101.

1.2.2. Não se aplica.

1.3. Participantes da ICP-Brasil

1.3.1. Autoridades Certificadoras

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

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

1.3.2. Autoridades de Registro

1.3.2.1. Os dados a seguir, referentes às Autoridades de Registro – AR utilizadas pela AC Certisign ICP-Brasil SSL para os processos de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são publicados em serviço de diretório e/ou em página web da AC Certisign ICP-Brasil SSL (http://icp-brasil.certisign.com.br/repositorio/ac_certisign_icp_br_ssl-ars.html):

a) relação de todas as AR credenciadas;

b) relação de AR que tenham se descredenciado da cadeia da AC Certisign ICP-Brasil SSL, com respectiva data do descredenciamento.

1.3.3. Titulares do 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 Certisign ICP-Brasil SSL e/ou por intermédio de suas AR é publicada em serviço de diretório e/ou em página web da AC Certisign ICP-Brasil SSL (http://icp-brasil.certisign.com.br/repositorio/ac_certisign_icp_br_ssl.html).

1.4. Usabilidade do Certificado

1.4.1 Uso apropriado 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 Certisign ICP-Brasil 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 Certisign ICP-Brasil 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 Os certificados de tipo A3 são utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.4.1.5 Não se aplica.

1.4.1.6 Não se aplica.

1.4.1.7 Não se aplica.

1.4.1.8 Não se aplica.

1.4.2 Uso proibitivo do certificado

Não se aplica.

1.5 Política de Administração

Neste item estão incluídos nome, endereço e outras informações da AC Certisign ICP-Brasil SSL, assim como são informados o nome, os números de telefone e o endereço eletrônico de uma pessoa para contato.

1.5.1 Organização administrativa do documento

Nome da AC: AC Certisign ICP-Brasil SSL

1.5.2 Contatos

Endereço: Rua Bela Cintra, 904 – 11. Andar – São Paulo - 01415-000

Telefone: (11) 4501-2215

Página web: http://icp-brasil.certisign.com.br/repositorio/ac_certisign_icp_br_ssl.html

E-mail: mailto: normas@certisign.com.br

1.5.3 Pessoa que determina a adequabilidade da DPC com a PC

Nome: Bruna Spirandelli

Área: Normas e Compliance

Telefone: (11) 4501-2526

E-mail: normas@certisign.com.br

1.5.4 Procedimentos de aprovação da PC

Esta PC é aprovada pelo ITI.

Os procedimentos de aprovação desta PC da AC Certisign ICP-Brasil SSL são estabelecidos a critério do CG da ICP-Brasil.

1.6 Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
AR	Autoridades de Registro

CEI	Cadastro Específico do INSS
CG ICP-Brasil	Comitê Gestor da ICP-Brasil
CN	*Common Name*
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CPF	Cadastro de Pessoas Físicas
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
EV	*Extended Validation*
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IEC	*International Electrotechnical Commission*
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	*International Organization for Standardization*
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
OU	*Organization Unit*
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado

PIS	Programa de Integração Social
PSBIO	Prestados de Serviço de Biometria
PSC	Prestador de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
RFC	*Request For Comments*
RG	Registro Geral
SSL	*Secure Socket Layer*
UF	Unidade de Federação
URL	*Uniform Resource Locator*

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

Nos itens seguintes são referidos os itens correspondentes da DPC da AC Certisign ICP-Brasil 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 DPC da AC Certisign ICP-Brasil SSL.

Nos itens seguintes são referidos os itens correspondentes da DPC da AC Certisign ICP-Brasil SSL.

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 DPC da AC Certisign ICP-Brasil 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

5.4.8. Avaliações de vulnerabilidade

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 Certisign ICP-Brasil 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.

Em quaisquer das situações, a geração do par de chaves criptográficas ocorre utilizando hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.

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

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

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

6.1.1.6. 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 tipo de certificado emitido pela AC Certisign ICP-Brasil SSL e descrito nesta PC é o A3.

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
A3	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO

Nota: Não se aplica.

6.1.2. Entrega da chave privada à entidade

Não se aplica.

6.1.3. Entrega da chave pública para emissor de certificado

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

6.1.4. Entrega de chave pública da AC às terceiras partes

A AC Certisign ICP-Brasil SSL disponibiliza o seu certificado, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, através de endereço Web:

Para G1:

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_Certisign_Icp_Br_Ssl_G1.p7c

Para G2:

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_Certisign_Icp_Br_Ssl_G2.p7c

Para G3:

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_Certisign_Icp_Br_Ssl_G3.p7c

Para G4:

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_Certisign_Icp_Br_Ssl_G4.p7c

6.1.5. Tamanhos de chave

6.1.5.1. O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC Certisign ICP-Brasil SSL é de 2048 bits.

6.1.5.2. Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo A3 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 e verificação da qualidade dos parâmetros

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, keyEncipherment ou keyAgreement.

Os pares de chaves correspondentes aos certificados emitidos pela AC Certisign ICP-Brasil SSL são utilizados para autenticação de servidores.

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 Certisign ICP-Brasil SSL.

6.2.1. Padrões e controle para módulo criptográfico

6.2.1.1. O módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão de homologação ICP-Brasil ou Certificação INMETRO.

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

A AC não realiza a recuperação (escrow) de chaves privadas de assinatura, isto é, não se permite que terceiros possam obter uma chave privada de assinatura sem o consentimento do titular do certificado.

6.2.4. Cópia de segurança de chave privada

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

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

6.2.4.3. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4. Não se aplica.

6.2.5. Arquivamento de chave privada

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

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

6.2.6. Inserção de chave privada em módulo criptográfico

Não se aplica.

6.2.7 Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

6.2.8. Método de ativação de chave privada

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

6.2.9. Método de desativação de chave privada

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

6.2.10. 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 dos titulares de certificados de assinatura digital e as LCR emitidas pela AC Certisign ICP-Brasil SSL permanecem armazenadas após a expiração dos correspondentes certificados, permanentemente, na forma da legislação em vigor, para verificação de assinaturas geradas durante seu período de validade.

6.3.2. Períodos de operação do certificado e períodos de uso para as chaves pública e privada

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

6.3.2.2. Não se aplica.

6.3.2.3. Não se aplica.

6.3.2.4. Não se aplica.

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 dos titulares de certificados possui conexão com o dispositivo de mídia inteligente e o respectivo driver instalado. A mídia inteligente possui processador criptográfico com capacidade de geração interna das chaves.

6.5.2. Classificação da segurança computacional

Não se aplica.

6.6. Controles Técnicos do Ciclo de Vida

A AC Certisign ICP-Brasil SSL desenvolve sistemas relacionadas ao ciclo de vida do certificado digital.

6.6.1. Controles de desenvolvimento de sistema

6.6.1.1. A AC Certisign ICP-Brasil 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 Certisign ICP-Brasil 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 Certisign ICP-Brasil SSL provêm documentação suficiente para suportar avaliações externas de segurança dos componentes da AC Certisign ICP-Brasil SSL.

6.6.2. Controles de gerenciamento de segurança

6.6.2.1. A AC Certisign ICP-Brasil 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 Certisign ICP-Brasil SSL utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

6.6.3. Controles de segurança de ciclo de vida

Não se aplica.

6.6.4 Controles na Geração de LCR

Antes de publicadas, todas as LCRs geradas pela AC Certisign ICP-Brasil 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

Não se aplica.

7. PERFIS DE CERTIFICADO, LCR E OCSP

Os itens seguintes especificam os formatos dos certificados e das LCR/OCSP gerados segundo esta PC, assim como informações sobre os padrões adotados, seus perfis, versões e extensões.

7.1. Perfil do Certificado

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

7.1.1. Número de versão

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

7.1.2. Extensões de certificado

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

a) **Authority Key Identifier**, não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da AC Certisign ICP-Brasil SSL;

b) **Key Usage,** crítica: configurados conforme disposto no item 7.1.2.7 deste documento;

c) **Certificate Policies**, não crítica, contém:

- O OID desta PC: 2.16.76.1.2.3.101;

- Os campos policyQualifiers contém o endereço *Web* da DPC AC Certisign ICP-Brasil SSL: http://icp-brasil.certisign.com.br/repositorio/dpc/ac_certisign_icp_br_ssl/DPC_AC_Certisign_Icp_Br_Ssl.pdf

Certificados de autenticação de servidor (SSL/TLS) contém ainda o OID da política de certificado de identificação dos requisitos do CA/B Forum Guidelines (2.23.140.1.1, se EV SSL ou 2.23.140.1.2.2, se OV SSL);

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

Para G1:

http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisignICPBRSSLG1/LatestCRL.crl

http://icp-brasil.outralcr.com.br/repositorio/lcr/ACCertisignICPBRSSLG1/LatestCRL.crl

Para G2:

http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisignICPBRSSLG2/LatestCRL.crl

http://icp-brasil.outralcr.com.br/repositorio/lcr/ACCertisignICPBRSSLG2/LatestCRL.crl

Para G3:

http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisignICPBRSSLG3/LatestCRL.crl

http://icp-brasil.outralcr.com.br/repositorio/lcr/ACCertisignICPBRSSLG3/LatestCRL.crl

Para G4:

http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisignICPBRSSLG4/LatestCRL.crl

http://icp-brasil.outralcr.com.br/repositorio/lcr/ACCertisignICPBRSSLG4/LatestCRL.crl

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

Para G1:

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_Certisign_Icp_Br_Ssl_G1.p7c

Para G2:

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_Certisign_Icp_Br_Ssl_G2.p7c

Para G3:

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_Certisign_Icp_Br_Ssl_G3.p7c

Para G4:

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_Certisign_Icp_Br_Ssl_G4.p7c

A segunda entrada contem o endereço de acesso ao serviço de Consulta On-Line de Situação de Certificado (On-line Certificate Status Protocol- OCSP): http://ocsp-ac-certisign-ICP-Br-ssl.certisign.com.br

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

7.1.2.2. A ICP-Brasil define como obrigatórias as seguintes extensões:

a) ***"Authority Key Identifier",*** **não crítica**: o campo keyIdentifier deve conter o *hash* SHA-1 da chave pública da AC;

b) ***"Key Usage",*** **crítica**: configurados conforme disposto no item 7.1.2.7 deste documento;

c) "***Certificate Policies",*** **não crítica**: deve conter o OID da PC correspondente e o endereço Web da DPC da AC que emite o certificado.

d) ***"CRL Distribution Points",*** **não crítica**: deve conter 02 (dois) endereços na Web onde se obtém a LCR correspondente;

e) **"*Authority Information Access*", não crítica:** A primeira entrada deve conter o método de acesso id-ad-caIssuer, utilizando um dos seguintes protocolos de acesso, HTTP, HTTPS ou LDAP, para a recuperação da cadeia de certificação. A segunda entrada deve conter o método de acesso id-ad-ocsp, com o respectivo endereço do respondedor OCSP, utilizando um dos seguintes protocolos de acesso, HTTP, HTTPS ou LDAP, para certificados de autenticação de servidor (SSL/TLS). Todos os outros tipos de certificado podem conter essa segunda entrada. Essas extensões somente são aplicáveis para certificados de usuário final.

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

a) Não se aplica.

b) Não se aplica.

c) Para certificado de equipamento, aplicação e OCSP:

c.1) Não se aplica.

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, exceto nos casos de certificado digital cuja titularidade foi validada pela AR de conselho de classe profissional;

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) Não se aplica.

7.1.2.5. Campos otherName adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidos pela AC Certisign ICP-Brasil 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 criticalidade conforme descrição abaixo:

a) Não se aplica

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: contem 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;

b.1) para certificados de Autenticação de Servidor (SSL/TLS) para o Open Banking:

“Key Usage”, crítica: somente os bits digitalSignature, keyEncipherment e/ou keyAgreement estão ativados;

“Extended Key Usage”, não crítica: contém o propósito client authentication OID = 1.3.6.1.5.5.7.3.2 e server authentication OID = 1.3.6.1.5.5.7.3.1;

b.2) para certificados de Autenticação de Servidor (SSL/TLS) para o Open Insurance:

“Key Usage”, crítica: somente os bits digitalSignature, keyEncipherment e/ou keyAgreement estão ativados;

“Extended Key Usage”, não crítica: contém o propósito client authentication OID = 1.3.6.1.5.5.7.3.2 e server authentication OID = 1.3.6.1.5.5.7.3.1;

c) Não se aplica.

d) Não se aplica.

e) para certificados de Assinatura de Resposta OCSP:

“Key Usage”, crítica: contem 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) Não se aplica.

g) Não se aplica.

7.1.3. Identificadores de algoritmo

Os certificados emitidos pela AC Certisign ICP-Brasil SSL 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#1.

7.1.4. Formatos de nome

7.1.4.1. Não se aplica.

7.1.4.2. Não se aplica.

7.1.4.3. Não se aplica.

7.1.4.4. O certificado digital emitido para autenticação de servidor (SSL/TLS) deverá adotar o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ)

CN = se presente, este campo deve conter um único nome de domínio pertencente ou controlado pelo titular

ST = unidade da federação do endereço físico do titular do certificado

L = cidade do endereço físico do titular

Business Category (OID 2.5.4.15) = tipo de categoria comercial, devendo conter:

"Private Organization" ou "Government Entity" ou "Business Entity" ou "Non-Commercial Entity"

SERIALNUMBER (OID 2.5.4.5) = CNPJ

Jurisdiction Country Name (OID: 1.3.6.1.4.1.311.60.2.1.3) = BR

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

7.1.4.4.1. O certificado digital emitido para autenticação de servidor (SSL/TLS), até 31/08/2022, para o Open Banking deverá adotar o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR (countryName (OID 2.5.4.6))

O = nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ) (organizationName (OID 2.5.4.10))

CN = se presente, este campo deve conter um único nome de domínio pertencente ou controlado pelo titular (commonName (OID 2.5.4.3))

ST = unidade da federação do endereço físico do titular do certificado (stateOrProvinceName (OID 2.5.4.8))

L = cidade do endereço físico do titular (localityName (OID 2.5.4.7))

Business Category = tipo de categoria comercial, devendo conter:

*"Private Organization" ou "Government Entity" ou "Business Entity" ou "Non-Commercial Entity" (*businessCategory (OID 2.5.4.15))

SERIALNUMBER = CNPJ (serialNumber (OID 2.5.4.5))

Jurisdiction Country Name = BR (jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3))

ORGANIZATIONAL UNIT NAME = Código de Participante associado ao CNPJ listado no Serviço de Diretório do Open Banking Brasil (organizationalUnitName (OID 2.5.4.11))

UID = Software Statement ID gerado pelo Diretório do Open Banking Brasil (UID (OID 0.9.2342.19200300.100.1.1))

7.1.4.4.2 O certificado digital emitido para autenticação de servidor (SSL/TLS), a partir de 01/09/2022, para o Open Banking deverá adotar o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR (countryName (OID 2.5.4.6))

O = nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ) (organizationName (OID 2.5.4.10))

CN = se presente, este campo deve conter um único nome de domínio pertencente ou controlado pelo titular (commonName (OID 2.5.4.3))

ST = unidade da federação do endereço físico do titular do certificado (stateOrProvinceName (OID 2.5.4.8))

L = cidade do endereço físico do titular (localityName (OID 2.5.4.7))

Business Category = tipo de categoria comercial, devendo conter:

*"Private Organization" ou "Government Entity" ou "Business Entity" ou "Non-Commercial Entity" (*businessCategory (OID 2.5.4.15))

SERIALNUMBER = CNPJ (serialNumber (OID 2.5.4.5))

Jurisdiction Country Name = BR (jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3))

organizationIdentifier = OFBBR-<Código de Participante> (OID 2.5.4.97)

UID = Software Statement ID gerado pelo Diretório do Open Banking Brasil (UID (OID 0.9.2342.19200300.100.1.1))

7.1.4.4.3 O certificado digital emitido para autenticação de servidor (SSL/TLS) para o Open Insurance Brasil deverá adotar o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR (countryName (OID 2.5.4.6))

O = nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ) (organizationName (OID 2.5.4.10))

CN = se presente, este campo deve conter um único nome de domínio pertencente ou controlado pelo titular (commonName (OID 2.5.4.3))

ST = unidade da federação do endereço físico do titular do certificado (stateOrProvinceName (OID 2.5.4.8))

L = cidade do endereço físico do titular (localityName (OID 2.5.4.7))

Business Category = tipo de categoria comercial, devendo conter:

*"Private Organization" ou "Government Entity" ou "Business Entity" ou "Non-Commercial Entity" (*businessCategory (OID 2.5.4.15))

SERIALNUMBER = CNPJ (serialNumber (OID 2.5.4.5))

Jurisdiction Country Name = BR (jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3))

organizationIdentifier = OPINBR-<Código de Participante> (OID 2.5.4.97)

UID = Software Statement ID gerado pelo Diretório do Open Insurance (UID (OID 0.9.2342.19200300.100.1.1))

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

7.1.5. Restrições de nome

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

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

a) não são admitidos sinais de acentuação, trema ou cedilhas;

b) além dos caracteres alfanuméricos, são utilizados somente os seguintes caracteres especiais:

Caractere	Código NBR9611 (hexadecimal)
branco	20

!	21
"	22
#	23
$	24
%	25
&	26
'	27
(	28
)	29
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A

;	3B
=	3D
?	3F
@	40
\	5C

7.1.6. OID (Object Identifier) de Política de Certificado

O OID desta PC é 2.16.76.1.2.3.101.

Todo certificado emitido segundo essa PC, PC A3 da AC Certisign ICP-Brasil 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

O campo policyQualifiers da extensão "Certificate Policies" contém o endereço web da DPC da AC Certisign ICP-Brasil SSL (http://icp-brasil.certisign.com.br/repositorio/dpc/ac_certisign_icp_br_ssl/DPC_AC_Certisign_Icp_Br_Ssl.pdf).

7.1.9. Semântica de processamento para as extensões críticas de PC

Extensões críticas são interpretadas conforme a RFC 5280.

7.2. Perfil de LCR

7.2.1. Número(s) de versão

As LCR geradas pela AC Certisign ICP-Brasil SSL 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 Certisign ICP-Brasil SSL e sua criticalidade.

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

a) **Authority Key Identifier**, não crítica: contém o hash SHA-1 da chave pública da AC Certisign ICP-Brasil SSL;

b) **CRL Number,** não crítica: contém um número sequencial para cada LCR emitida pela AC Certisign ICP-Brasil SSL.

7.3. Perfil de OCSP

7.3.1. Número(s) de versão

Os serviços de respostas OCSP da AC Certisign ICP-Brasil 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 Certisign ICP-Brasil 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 Certisign ICP-Brasil 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 Certisign ICP-Brasil 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 serão solicitadas e/ou definidas pelo Grupo de Práticas e Políticas da AC Certisign ICP-Brasil SSL. A aprovação e consequente adoção de nova versão serão sujeitas à autorização da AC Raiz. Qualquer alteração na PC deverá ser submetida à aprovação da AC Raiz.

9.12.2. Mecanismo de notificação e períodos

A AC Certisign ICP-Brasil SSL mantém página específica com a versão corrente desta PC para consulta pública, a qual está disponibilizada no endereço Web http://icp-brasil.certisign.com.br/repositorio/pc/ac_certisign_icp_br_ssl/PC_AC_Certisign_Icp_Br_Ssl_A3.pdf.

9.12.3. Circunstâncias na qual o OID deve ser alterado

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 Certisign ICP-Brasil 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.

9.16.2. Cessão

9.16.3. Independência de disposições

9.16.4. Execução (honorários dos advogados e renúncia de direitos)

9.17. Outras provisões

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

Novas versões serão igualmente submetidas à aprovação da AC Raiz.

10. DOCUMENTOS REFERENCIADOS

10.1. 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
[1]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL Aprovado pela Resolução nº 132, de 10 de novembro de 20017	DOC-ICP-17
[2]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL Aprovado pela Resolução nº 59, de 28 de novembro de 2008	DOC-ICP-12
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 06, de 22 de novembro de 2001	DOC-ICP-03

11. REFERÊNCIAS BIBLIOGRÁFICAS

RFC 3647, IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, november 2003.

RFC 5280, IETF - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, may 2008.

RFC 2818, IETF - HTTP Over TLS, may 2000.

RFC 6960, IETF - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, june 2003