Declaração de Práticas de Certificação da Autoridade de Registro USODIGITAL, Vinculada à AC DOCCLOUD RFB.

[DPC da AR USODIGITAL]

Versão 1.0 de 27.07.2020

SUMÁRIO

CONTROLE DE ALTERAÇÕES

RESPONSÁVEL	APROVAÇÃO	DESCRIÇÃO DA ALTEAÇÃO	VERSÃO	DATA
Compliance	Versão Inicial		1.0	27.07.2020

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. Esta Declaração de Práticas de Certificação (DPC) descreve as práticas e os procedimentos empregados pelas Autoridades de Registro enquanto credenciadas na Estrutura de Certificação de Digital da Autoridade Certificadora DOCCLOUD para a Secretaria da Receita Federal do Brasil (AC DOCCLOUD RFB) integrante na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) na execução dos seus serviços de certificação digital.

1.1.2. A AC DOCCLOUD RFB mantém atualizada esta Declaração de Práticas de Certificação de AR atualizada.

1.1.2. A AC DOCCLOUD RFB está certificada em nível imediatamente subsequente ao da Autoridade Certificadora da Secretaria da Receita Federal do Brasil (AC-RFB) certificada pela AC Raiz da ICP-Brasil. O certificado da AC DOCCLOUD RFB contém a chave pública correspondente à sua chave privada, utilizada para assinar certificados de assinatura geral e proteção de e-mail (S/MIME): de assinatura A1 e A3 (para pessoas físicas, jurídicas e aplicação para assinatura de resposta OCSP) e para assinar a sua Lista de Certificados Revogados (LCR).

1.2. NOME DO DOCUMENTO E IDENTIFICAÇÃO

Este documento é chamado “Declaração de Práticas de Certificação da Autoridade de Registro USODIGITAL vinculada à AC DOCCLOUD RFB” e comumente referido como “DPC da AR USODIGITAL”.

1.3. PARTICIPANTES DA ICP-BRASIL

1.3.1. Autoridades de Registro

Os dados a seguir, referentes às Autoridades de Registro – AR utilizadas pela AC DOCCLOUD RFB 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 https://www.acdoccloud.com.br/repositorio com a seguintes informações:

a) relação de todas as AR credenciadas; e
c) relação de AR que tenham se descredenciado da cadeia da AC DOCCLOUD RFB, com respectiva data do descredenciamento.

1.3.2. Titulares de Certificado

Pessoas físicas ou jurídicas inscritas no CPF ou no CNPJ podem ser Titulares de Certificado e-CPF ou e-CNPJ Tipo A1 e A3, desde que não enquadradas na situação cadastral de CANCELADA ou NULA (pessoa física) ou na condição de BAIXADA, INAPTA, SUSPENSA ou NULA (pessoa jurídica), conforme o disposto nos incisos I e II do art. 6. da Instrução Normativa RFB n. 1077, de 29 de Outubro de 2010 e Anexo I da Portaria RFB / Sucor / Cotec nº 18, de 19 de fevereiro de 2019 (Leiaute dos Certificados Digitais da Secretaria da Receita Federal do Brasil - Versão 4.4).

No caso de certificado emitido para equipamento, o titular será a pessoa jurídica solicitante do certificado. No caso de certificado emitido para aplicação, o titular será a pessoa jurídica solicitante do

certificado. No caso de certificado emitido para pessoa jurídica, é designada pessoa física como responsável pelo certificado, que será a detentora da chave privada. Obrigatoriamente, o Responsável pelo certificado é o mesmo responsável pela pessoa jurídica cadastrado no CNPJ da RFB.

No caso de certificado emitido para aplicação, o titular será a pessoa jurídica solicitante do certificado.

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
Os Prestadores de Serviços de Suporte – PSS, Prestadores de Serviços Biométricos – PSBios e Prestadores de Serviços de Confiança - PSC vinculados à AC DOCCLOUD RFB estão relacionados em sua página web www.acdoccloud.com.br

1.3.5.1 PSS, PSBios ou PSC são entidades utilizadas pela AC DOCCLOUD RFB ou pelas ARs vinculadas para desempenhar atividade descrita nesta DPC ou na PC e se classificam em três categorias, conforme o tipo de atividade prestada:

a) disponibilização de infraestrutura física e lógica;
b) disponibilização de recursos humanos especializados; ou
c) disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

1.4. POLÍTICA DE ADMINISTRAÇÃO

Neste item estão incluídos nome, endereço e outras informações da **AR USODIGITAL** assim como são informados o nome, os números de telefone e o endereço eletrônico de uma pessoa para contato.

1.4.1. Organização administrativa do documento
NOME DA AR: AR USODIGITAL
RAZÃO SOCIAL: USO DIGITAL EIRELI.
LINK DE ACESSO: www.acdoccloud.com.br/repositorio

1.4.2. Contatos
Endereço: AVENIDA ENGENHEIRO CARLOS BERRINI, 1140, 7º ANDAR – CIDADE MOÇÕES – CEP: 04.571-000 – SÃO PAULO/SP.
Telefone: (11) 4020-8283

1.4.3. Adequabilidade desta DPC
AC DOCCLOUD RFB
Contato: NORMAS & COMPLIANCE
Telefone: (19) 3477-1144
E-mail: complianceac@doccloud.com.br

1.4.4. Procedimentos de aprovação desta DPC
Este documento foi analisado pela alta gestão da AC DOCCLOUD RFB e submetido ao Instituto de Tecnologia da Informação – ITI para aprovação. Os procedimentos de aprovação da DPC da AC DOCCLOUD RFB são estabelecidos a critério do CG da ICP-Brasil.

1.4.5. Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ACME	Automatic Certificate Management Environment
AC RAIZ	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridade de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CMVP	Cryptographic Module Validation Program
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COSO	Comitee of Sponsoring Organizations
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
EV	Extended Validation (WebTrust for Certification Authorities)
ICP-BRASIL	Infraestrutura de Chaves Públicas Brasileira
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IETF PKIX	Internet Engineering Task Force - Public-Key Infrastructured (X.509)
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	International Organization for Standardization
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	National Institute of Standards and Technology
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
OM-BR	Objetos Metrológicos ICP-Brasil
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	Proof of Possession
PS	Política de Segurança
PSBIO	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PSS	Prestador de Serviço de Suporte
RFC	Request For Comments
RG	Registro Geral
SAT	Sistema de Autenticação e Transmissão

SINRIC	Sistema Nacional de Registro de Identificação Civil
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCSEC	Trusted System Evaluation Criteria
TSDM	Trusted Software Development Methodology
UF	Unidade de Federação
URL	Uniform Resource Locator

2. IDENTIFICAÇÃO E AUTENTICAÇÃO

À **AR USODIGITAL** verifica a autenticidade da identidade e/ou atributos de pessoas físicas e jurídicas da ICP-Brasil antes da inclusão desses atributos em um certificado digital. As pessoas físicas e jurídicas estão proibidas de usar nomes em seus certificados que violem os diretos de propriedade intelectual de terceiros.

À AC DOCCLOUD RFB e sua AR credenciada reserva o direito, sem responsabilidade a qualquer solicitante, de rejeitar os pedidos.

2.1. ATRIBUIÇÕES DE NOMES

2.1.1. Tipos de nomes

2.1.1.1. O tipo de nome admitido para os titulares de certificados emitidos, segundo esta DPC, é o “distinguished name” do padrão ITU X.500, endereços de correio eletrônico, endereço de página Web (URL), ou outras informações que permitam a identificação unívoca do titular.

2.1.1.2. Um certificado emitido para uma AC subsequente não deverá incluir o nome da pessoa responsável.

2.1.2. Necessidade de nomes serem significativos

2.1.2.1. Os certificados emitidos pela AC DOCCLOUD RFB exigem o uso de nomes significativos que possibilitam determinar univocamente a identidade da pessoa ou da organização titular do certificado a que se referem, para a identificação dos titulares dos certificados emitidos pela AC responsável.

2.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado

Item não aplicável.

2.1.4. Regras para interpretação de vários tipos de nomes

Item não aplicável.

2.1.5. Unicidades de nomes

Esta DPC estabelece que identificadores do tipo "Distinguished Name" (DN) são únicos para cada entidade titular de certificado emitido pela AC DOCCLOUD RFB.

Para assegurar a unicidade do campo dos certificados e-CNPJ e e-CPF é incluído o número do CNPJ e o número do CPF após o nome do titular do certificado, respectivamente, nos certificados e-CNPJ e e-CPF.

2.1.6. Procedimento para resolver disputa de nomes

No âmbito da AC não há disputa decorrente da igualdade de nomes entre solicitantes de certificados, pois o nome do Titular do Certificado será formado a partir do nome constante dos cadastros da RFB, CPF ou CNPJ para certificados de pessoa física ou jurídica respectivamente, acrescido do número de inscrição nestes cadastros. Este procedimento garante a unicidade de todos os nomes no âmbito da AC.

A AC DOCCLOUD RFB se reserva o direito de tomar todas as decisões na hipótese de haver disputa de nomes decorrentes da igualdade de nomes entre solicitantes diversos de certificados. Durante o processo de confirmação de identidade, cabe à entidade solicitante do certificado provar o seu direito de uso de um nome específico.

2.1.7. Reconhecimento, autenticação e papel de marcas registradas
Os processos de tratamento, reconhecimento e confirmação de autenticidade de marcas registradas serão executados de acordo com a legislação em vigor.

2.2. VALIDAÇÃO INICIAL DE IDENTIDADE

Neste e nos itens seguintes estão descritos em detalhes os requisitos e procedimentos utilizados pelas AR vinculadas a AC DOCCLOUD RFB para a realização dos seguintes processos:

a) IDENTIFICAÇÃO DO TITULAR DO CERTIFICADO – compreende as etapas abaixo, realizadas mediante a presença física do interessado, com base nos documentos de identificação citados nos itens 3.2.2, 3.2.3 e 3.2.7:

i. Confirmação da Identidade de um Indivíduo: comprovação de que a pessoa que se apresenta como titular do certificado de pessoa física é realmente aquela cujos dados constam na documentação e/ou biometria apresentada, vedada qualquer espécie de procuração para tal fim. No caso de pessoa jurídica, comprovar que a pessoa física que se apresenta como a sua representante é realmente aquela cujos dados constam na documentação apresentada, admitida a procuração apenas se o ato constitutivo previr expressamente tal possibilidade, devendo-se, para tanto, revestir-se da forma pública, com poderes específicos para atuar perante a ICP-Brasil e com prazo de validade de até 90 (noventa) dias. O responsável pela utilização do certificado digital de pessoa jurídica deve comparecer presencialmente, vedada qualquer espécie de procuração para tal fim.

ii. Confirmação da Identidade de uma Organização: comprovação de que os documentos apresentados se referem efetivamente à pessoa jurídica titular do certificado e de que a pessoa que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição;

iii. Emissão do Certificado: conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC DOCCLOUD RFB.

A extensão Subject Alternative Name é considerada fortemente relacionada à chave pública contida no certificado, assim, todas as partes dessa extensão devem ser verificadas, devendo o solicitante do certificado comprovar que detém os direitos sobre essas informações junto aos órgãos competentes, ou que está autorizado pelo titular da informação a utilizá-las.

2.2.1. Método para comprovar a posse de chave privada
A AR's vinculadas à AC DOCCLOUD RFB verifica se a entidade que solicita o certificado possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital. As RFC 4210 e 6712 são utilizadas como referência para essa finalidade.

No caso em que sejam requeridos procedimentos específicos para as PCs implementadas, eles são descritos nessas PCs, no item correspondente.

2.2.2. Autenticação da identidade de uma organização

2.2.2.1. Disposições Gerais

2.2.2.1.1. Neste item são definidos os procedimentos empregados pelas AR vinculadas para a confirmação da identidade de uma pessoa jurídica.

2.2.2.1.2. Em sendo o titular do certificado pessoa jurídica, é designada pessoa física como responsável pelo certificado, que será a detentora da chave privada. Obrigatoriamente, o responsável pelo certificado é o mesmo responsável pela pessoa jurídica cadastrado no CNPJ da RFB.

2.2.2.1.3. Deverá ser feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

a) apresentação do rol de documentos elencado no item 2.2.2.2;
b) apresentação do rol de documentos elencados no item 2.2.2.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo certificado;
c) presença física dos representantes legais, admitida a representação por procuração, conforme disposto no item 2.2, alínea 'a', inciso (i), e do responsável pelo uso do certificado; e
d) assinatura digital do termo de titularidade de que trata o item 4.1 pelo titular ou responsável pelo uso do certificado.

Nota 1: A AR poderá solicitar uma assinatura manuscrita ao requerente ou responsável pelo uso do certificado em termo específico para a comparação com o documento de identidade ou contrato social. Nesse caso, o termo manuscrito digitalizado e assinado digitalmente pelo AGR será apensado ao dossiê eletrônico do certificado, podendo o original em papel ser descartado.

2.2.2.1.4. Fica dispensado o disposto no item 3.2.2.1.3, alíneas "b" e "c" caso o responsável pelo certificado possua certificado digital de pessoa física ICP-Brasil válido, do tipo A3 ou superior, com os dados biométricos devidamente coletados, e a verificação dos documentos elencados no item 3.2.2.2 possa ser realizada eletronicamente por meio de barramento ou aplicação oficial.

2.2.2.2. Documentos para efeitos de identificação de uma organização

A confirmação da identidade de uma pessoa jurídica deverá ser feita mediante a apresentação de, no mínimo, os seguintes documentos:

a) Relativos à sua habilitação jurídica:

i. se pessoa jurídica cuja criação se deu ou foi autorizada por lei, cópia do ato constitutivo e CNPJ;

ii. se entidade privada:
1) Ato constitutivo, devidamente registrado no órgão competente ou Certidão Simplificada da Junta Comercial do seu registro; e
2) Documentos da eleição de seus administradores, quando aplicável;

b) relativos à sua habilitação fiscal:
i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou
ii. prova de inscrição no Cadastro Específico do INSS – CEI.

Nota 1: Essas confirmações que tratam o item 3.2.2.2 poderão ser feitas de forma eletrônica, desde que em barramentos ou aplicações oficiais de órgão competente. É obrigatório essas validações constarem no dossiê eletrônico do titular do certificado.

2.2.2.3. Informações contidas no certificado emitido para um indivíduo

2.2.2.3.1 É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa jurídica,

com as informações constantes nos documentos apresentados:

a) Nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ), sem abreviações;
b) Cadastro Nacional de Pessoa Jurídica (CNPJ);
c) Nome completo do responsável pelo certificado, sem abreviações; e
d) Data de nascimento do responsável pelo certificado.4 3.2.2.3.2

2.2.2.3.2 Cada PC pode definir como obrigatório o preenchimento de outros campos, ou o responsável pelo certificado, a seu critério e mediante declaração expressa no termo de titularidade, poderá solicitar o preenchimento de campos do certificado com suas informações pessoais, conforme item 2.2.3.2.

2.2.3. Autenticação da identidade de um indivíduo

A confirmação da identidade de um indivíduo é realizada mediante a presença física ou por ferramenta de videoconferência, com nível de segurança equivalente e observada pelas normas técnicas da ICP-Brasil do interessado, com base em documentos pessoais de identificação legalmente aceitos e pelo processo de identificação biométrica ICP-Brasil.

2.2.3.1. Documentos para efeitos de identificação de um indivíduo

Deverá ser apresentada a seguinte documentação, em sua versão original, para fins de identificação de indivíduo solicitante de certificado:

a) Registro de Identidade ou Passaporte, se brasileiro;
b) Título de Eleitor, com foto; ou
c) Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil;
d) Passaporte, se estrangeiro não domiciliado no Brasil;
e) Fotografia da face do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [11]; e
f) Impressões digitais do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [11].

NOTA 01: Entende-se como registro de identidade os documentos oficiais, físicos ou digitais, conforme admitido pela legislação específica, emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia.

2.2.3.1.1 Na hipótese de identificação positiva por meio do processo biométrico da ICP-Brasil fica dispensada a apresentação de qualquer dos documentos elencados no item e da etapa de verificação. As evidências desse processo farão parte do dossiê eletrônico do requerente.

2.2.3.1.2 Os documentos digitais deverão ser verificados por meio de barramentos ou aplicações oficiais dos entes federativos. Tal verificação fará parte do dossiê eletrônico do titular do certificado. Na hipótese da identificação positiva, fica dispensada a etapa de verificação conforme o item 2.2.3.1.3.

2.2.3.1.3 Os documentos em papel, os quais não existam formas de verificação por meio de barramentos ou aplicações oficiais dos entes federativos, deverão ser verificados:

a) por agente de registro distinto do que realizou à etapa de identificação;
b) na sede da AR ou AR própria da AC; e
c) antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

2.2.3.1.4 A emissão de certificados em nome dos absolutamente incapazes e dos relativamente incapazes observará o disposto na lei vigente, e as normas editadas pelo Comitê Gestor da ICP-Brasil.

2.2.3.1.5 Para à identificação de indivíduo na emissão de certificado digital para servidor público da ativa e militar da União, deverá ser observado o disposto item 3.2.9.3.

2.2.3.1.6 É facultado aos Bancos Múltiplos e Caixa Econômica Federal autorizados a funcionar pelo BACEN, na identificação de titulares pessoa física de conta de depósito, e as serventias extrajudiciais autorizadas a funcionar pelo Conselho Nacional de Justiça, utilizar o recurso disposto no item 2.2.9.4.

2.2.3.2 Informações contidas no certificado emitido para um indivíduo.
2.2.3.2.1 É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa física com as informações constantes nos documentos apresentados:

a) Cadastro de Pessoa Física (CPF);
b) nome completo, sem abreviações; e
c) data de nascimento.

2.2.3.2.2 Cada PC das Autoridades Certificadoras subsequentes à AC DOCCLOUD RFB pode definir como obrigatório o preenchimento de outros campos, ou o titular do certificado, a seu critério e mediante declaração expressa no termo de titularidade, poderá solicitar o preenchimento de campos do certificado com as informações constantes nos seguintes documentos:

a) número de Identificação Social NIS (PIS, PASEP ou CI);
b) número do Registro Geral RG do titular e órgão expedidor;
c) número do Cadastro Específico do INSS (CEI);
d) número do Título de Eleitor; Zona Eleitoral; Seção; Município e UF do Título de Eleitor;
e) número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente; e
f) documento assinado pela empresa com o valor do campo de login (UPN).

2.2.3.2.3 Para tanto, o titular deverá apresentar a documentação respectiva, caso a caso, em sua versão original.

Nota 1: É permitida a substituição dos documentos elencados acima por documento único, desde que este seja oficial e contenha as informações constantes daqueles.

Nota 2: O cartão CPF poderá ser substituído por consulta à página da Receita Federal Brasileira, devendo a cópia da mesma ser arquivada junto à documentação, para fins de auditoria.

2.2.4 Informações não verificadas do titular do certificado
Item não aplicável.

2.2.5 Validação das Autoridades
Na emissão de certificado de AC subsequente é verificado se a pessoa física é o representante legal da AC.

2.2.6 Critérios para interoperação
Item não aplicável.

2.2.7 Autenticação da identidade de equipamento ou aplicação
Item não aplicável

2.2.7.2 Procedimentos para efeitos de identificação de um equipamento ou aplicação
Item não aplicável

2.2.7.3 Informações contidas no certificado emitido para um equipamento ou aplicação
Item não aplicável

2.2.7.4 Autenticação de identificação de equipamento para certificado CF-e-SAT
Item não aplicável

2.2.7.5 Procedimentos para efeitos de identificação de um equipamento SAT
Item não aplicável

2.2.7.6 Informações contidas no certificado emitido para um equipamento SAT
Item não aplicável

2.2.7.7 Autenticação de identificação de equipamentos para certificado OM-BR
Item não aplicável

2.2.7.8 Procedimentos para efeitos de identificação de um equipamento metrológico
Item não aplicável

2.2.7.9 Informações contidas no certificado emitido para um equipamento metrológico
Item não aplicável

2.2.8 Procedimentos complementares
2.2.8.1 A AC mantém políticas e procedimentos internos que são revisados regularmente a fim de cumprir os requisitos dos vários programas de raiz dos quais a AC é membro, bem como os Requisitos de Linha de Base, as Diretrizes de EV para SSL e as Diretrizes de Assinatura de Código EV.

2.2.8.2 Todo o processo de identificação do titular do certificado deve ser registrado com verificação biométrica e assinado digitalmente pelos executantes, na solução de certificação disponibilizada pela AC com a utilização de certificado digital ICP-Brasil no mínimo do tipo A3. O sistema biométrico da ICP-BRASIL deve solicitar aleatoriamente qual dedo o AGR deve apresentar para autenticação, o que exige a inclusão de todos os dedos dos AGR no cadastro do sistema biométrico. Tais registros devem ser feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

2.2.8.3 Deve ser mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias poderão ser mantidas em papel ou em forma digitalizada, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1].

2.2.8.3.1 Item não aplicável.

2.2.8.4 A AC disponibiliza, para todas as AR vinculadas a sua respectiva cadeia, uma interface para verificação biométrica do requerente junto ao Sistema Biométrico da ICP-Brasil, em cada processo de emissão de um certificado digital ICP-Brasil, conforme estabelecido no DOC-ICP-03 [6] e DOC-ICP-05.02 [10].

2.2.8.4.1 Na hipótese de identificação positiva no processo biométrico da ICP-brasil, fica dispensada a apresentação de qualquer documentação de identidade do requerente ou da etapa de verificação conforme item 2.2.3.1.

2.2.9 Procedimentos específicos
Item não aplicável.

2.2.9.1 Disposições para a Validação de Solicitação de Certificados do Tipo A CF-e-SAT:
Item não aplicável.

2.2.9.5 Disposições para a Validação de Solicitação de Certificados do Tipo OM-BR:
Item não aplicável

2.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES

2.3.1 Identificação e autenticação para rotina de novas chaves antes da expiração
2.3.1.1 No item seguinte estão estabelecidos os processos de identificação do solicitante pela AC DOCCLOUD RFB para a geração de novo par de chaves, e de seu correspondente certificado, antes da expiração de um certificado vigente.
2.3.1.2Esse processo poderá ser conduzido segundo uma das seguintes possibilidades:

a) adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado;
b) a solicitação por meio eletrônico, assinada digitalmente com o uso de certificado vigente que seja pelo menos do mesmo nível de segurança, limitada a 1 (uma) ocorrência sucessiva, permitida tal hipótese apenas para os certificados digitais de pessoa física;
c) por meio de mecanismo automatizado de gerenciamento de certificado do tipo SSL/TLS (ACME), conforme disposto no item 2.3.1.2.1.

2.3.1.2.1 Para certificados de equipamento ou aplicação que utilizem URL, à AC poderá implementar mecanismos automatizado de gerenciamento de certificado (ACME) de forma a preservar a posse ou propriedade da URL (domínio) e à identificação do solicitante, seja pessoa física ou jurídica. O processo automatizado implica as seguintes etapas:

a) o solicitante submete uma requisição de certificado (PKCS#10) da URL desejada;
b) a requisição deverá ser acompanhada do certificado da URL solicitada, ainda válido, e o conjunto (requisição + certificado da URL) deve ser assinado com certificado ICP-Brasil, no mínimo do tipo A3, de pessoa física ou jurídica do responsável pelo domínio. Se o responsável pelo domínio for pessoa física, o signatário deve ser o mesmo contido no campo otherName (OID 2.16.76.1.3.2) que identifica o responsável pelo certificado da URL. Se o responsável pelo domínio for pessoa jurídica, o signatário deve ser um certificado de pessoa jurídica cujo CNPJ seja o mesmo contido no campo otherName (OID 2.16.76.1.3.3) que identifica o titular do certificado da URL;
c) o aplicativo de AR valida a assinatura e a requisição e, caso esteja em conformidade, encaminha desafio de prova de domínio e o termo de titularidade;
d) o solicitante responde o desafio e assina o termo de titularidade com o mesmo certificado utilizado no item “b”, acima;
e) confirmado atendimento pleno do desafio e da assinatura do termo de titularidade, o aplicativo de AR poderá emitir o certificado e encaminhá-lo ao solicitante; e
f) todas as evidências do processo acima devem constar no dossiê do certificado.

2.3.1.3 Caso sejam requeridos procedimentos específicos para as PC implementadas, os mesmos devem ser descritos nessas PC, no item correspondente.

2.3.1 Identificação e autenticação para novas chaves após a revogação

2.3.2.1. Após a revogação ou expiração do certificado, os procedimentos utilizados para confirmação da identidade do solicitante de novo certificado são os mesmos exigidos na solicitação inicial do certificado, na forma e prazo descritos nas PC implementadas.

2.3.2.2. Para o caso específico de revogação de um certificado de AC de nível imediatamente subsequente ao da AC responsável pela DPC, este item deve estabelecer que, após a expiração ou revogação de seu certificado, aquela AC deverá executar os processos regulares de geração de seu novo par de chaves.

2.4 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO

A solicitação de revogação de certificado é realizada através de formulário específico, permitindo a identificação inequívoca do solicitante.

A confirmação da identidade do solicitante é feita com base na confrontação de dados fornecidos na solicitação de revogação e os dados previamente cadastrados na AR. As solicitações de revogação de certificado são registradas. O procedimento para solicitação de revogação de certificado emitido pela AC DOCCLOUD RFB está descrito no item 3.9.3.

Solicitações de revogação de certificados devem ser registradas.

3. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

3.1 Solicitação do certificado

3.1.1. Neste item são descritos todos os requisitos e procedimentos operacionais estabelecidos pela AC DOCCLOUD RFB e pelas ARs a ela vinculadas para as solicitações de emissão de certificado. Esses requisitos e procedimentos compreendem todas as ações necessárias tanto do indivíduo solicitante quanto das AC e AR no processo de solicitação de certificado digital e contemplam:

a) a comprovação de atributos de identificação constantes do certificado, conforme item 3.2;
b) o uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes ao de um certificado de tipo A3, a autenticação biométrica do agente de registro responsável pelas solicitações de emissão e de revogação de certificados; ou quando da emissão para servidores públicos da ativa e militares da União, Estados e Distrito Federal, por servidor público e militar autorizado pelos sistemas de gestão de pessoal dos órgãos competentes; e
c) um termo de titularidade assinado digitalmente pelo titular do certificado ou pelo responsável pelo uso do certificado, no caso de certificado de pessoa jurídica, conforme o adendo referente ao TERMO DE TITULARIDADE [4] específico, e, ainda, quando emissão para servidor público da ativa e militar da União, Estados e Distrito Federal pela autoridade designada formalmente pelos órgãos competentes.

Nota 1: o termo de titularidade para certificados de usuários finais com propósito de uso EV SSL e EV CS deve seguir o padrão adotado no documento EV SSL e EV CS Guidelines.

Nota 2: na impossibilidade técnica de assinatura digital do termo de titularidade (como certificados SSL, de equipamento, aplicação, codesign, carimbo de tempo e outros que façam uso de CSR) será aceita a assinatura manuscrita do termo ou assinatura digital do termo com o certificado ICP-Brasil do titular do certificado ou responsável pelo uso do certificado, no caso de certificado de pessoa jurídica. No caso de assinatura manuscrita do termo será necessária a verificação da assinatura contra o documento de identificação.

Nota 3: durante o período de transição previsto na resolução 151, de 30 de maio de 2019, que se encerra em 12/10/2019, será aceita a assinatura manuscrita do termo (i) pelo titular do certificado, para certificados de pessoa física, e (ii) pelo titular e responsável pelo uso do certificado, para certificados de pessoa jurídica. Em ambos os casos, no momento da identificação presencial, será necessária a verificação da(s) assinatura(s) contra o documento de

identificação.

3.1.1 Quem pode submeter uma solicitação de certificado
A submissão da solicitação deve ser sempre por intermédio da AR.

3.1.1.1. A solicitação de certificado para AC de nível imediatamente subsequente ao da AC DOCCLOUD RFB somente será possível após o processo de credenciamento e a autorização de funcionamento da AC em questão, conforme disposto pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

3.1.1.2. A solicitação de certificado para equipamento de carimbo do tempo de Autoridade de Carimbo do Tempo (ACT) credenciada na ICP-Brasil somente será possível após a notificação do deferimento do credenciamento, conforme disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].
3.1.1.3 Nos casos previstos no item 3.1.1.1, a AC subsequente deverá encaminhar a solicitação de certificado à AC emitente por meio de seus representantes legais, utilizando o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

3.1.1.4 A solicitação de um certificado de AC de nível imediatamente subsequente deve ser feita pelos seus representantes legais.

3.1.2 Processo de registro e responsabilidades
Abaixo são descritas as obrigações gerais das Autoridades de Registro. Caso haja obrigações específicas para as PCs implementadas, as mesmas devem ser descritas nessas PCs, no item correspondente.

3.1.2.3 Responsabilidades da AR
A AR será responsável pelos danos a que der causa.

3.1.2.4 As obrigações das AR's
As obrigações das ARs vinculadas à AC DOCCLOUD RFB são as abaixo relacionadas:

a) receber solicitações de emissão ou de revogação de certificados;
b) confirmar a identidade do solicitante e a validade da solicitação;
c) encaminhar a solicitação de emissão ou de revogação de certificado, por meio de acesso remoto ao ambiente de AR hospedado nas instalações da AC responsável utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICPBRASIL [1];
d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
e) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC vinculada e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1], bem como Princípios e Critérios WebTrust para AR [14];
f) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
g) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 2.2.2, 2.2.3 e 2.2.7; e
h) divulgar suas práticas, relativas à cada cadeia de AC ao qual se vincular, em conformidade com o documento Princípios e Critérios WebTrust para AR [14].

3.2 PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO

3.2.1 Execução das funções de identificação e autenticação
À AC DOCCLOUD RFB e suas e AR DOCCLOUD executam as funções de identificação e autenticação conforme item 3 desta DPC.

3.2.1.1 À AC DOCCLOUD RFB e AR DOCCLOUD podem, com a devida justificativa formal, aceitar ou rejeitar pedidos de certificados de requerentes de acordo com os procedimentos descritos nesta DPC.

3.2.3 Tempo para processar a solicitação de certificado

À AC DOCCLOUD RFB cumprirá os procedimentos determinados na ICP-Brasil. Não haverá tempo máximo para processar as solicitações na ICP-Brasil.

3.3 EMISSÃO DE CERTIFICADO

3.3.1 Ações das Autoridades de Registro durante à emissão de um certificado

3.3.1.1 A emissão de certificado depende do correto preenchimento de formulário de solicitação, da assinatura do "Termo de Titularidade", no caso de certificados de pessoas jurídicas, ou aplicações e dos demais documentos exigidos. Após o processo de validação das informações fornecidas pelo solicitante, o certificado é emitido e Titular é notificado da emissão e do método para a retirada do certificado.

3.3.1.2 O certificado é considerado válido a partir do momento de sua emissão.

4. CONTROLES DE SEGURANÇA COMPUTACIONAL

4.1. Controle de segurança para as Autoridades de Registro

4.1.1. Neste item estão descritos os requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pelas AR para os processos de validação e aprovação de certificados.

4.1.2. Os requisitos abaixo correspondem aos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1]:

a) controle de acesso lógico ao sistema operacional;
b) exigência de uso de senhas fortes;
c) diretivas de senha e de bloqueio de conta;
d) logs de auditoria do sistema operacional ativados, registrando:
    i. iniciação e desligamento do sistema;
    ii. tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AR;
    iii. mudanças na configuração da estação;
    iv. tentativas de acesso (login) e de saída do sistema (logoff);
    v. tentativas não autorizadas de acesso aos arquivos de sistema;
    vi. tentativas de iniciar, remover, habilitar e desabilitar usuários e de atualizar e recuperar suas chaves
e) antivírus, antitrojan e antispyware, instalados, atualizados e habilitados;
f) firewall pessoal ativado, com permissões de acesso mínimas necessárias às atividades, podendo esse ser substituído por firewall corporativo, para equipamentos instalados em redes que possuam esse dispositivo;
g) proteção de tela acionada no máximo após dois minutos de inatividade e exigindo senha do usuário para desbloqueio;
h) sistema operacional mantido atualizado, com aplicação de correções necessárias (patches, hotfix, etc.);
i) utilização apenas de softwares licenciados e necessários para a realização das atividades do usuário;
j) impedimento de login remoto, via outro equipamento ligado à rede de computadores utilizada pela AR, exceto para as atividades de suporte remoto;
k) utilização de data e hora de Fonte Confiável do Tempo (FCT).

5. CONFORMIDADE COM A LEI APLICÁVEL

A AC DOCCLOUD RFB está sujeita à Legislação que lhe é aplicável, comprometendo-se a cumprir e a observar as obrigações e direitos previstos em Lei.

5.1. DISPOSIÇÕES DIVERSAS

5.1.1. Acordo completo

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

5.1.2. Cessão

Os direitos e obrigações previstos nesta DPC são de ordem pública e indisponíveis, não podendo ser cedidos ou transferidos a terceiros.

5.1.3. Independência de disposições

A invalidade, nulidade ou ineficácia de qualquer das disposições desta DPC não prejudicará as demais disposições, as quais permanecerão plenamente válidas e eficazes. Neste caso a disposição inválida, nula ou ineficaz será considerada como não escrita, de forma que esta DPC será interpretada como se não contivesse tal disposição, e na medida do possível, mantendo a intenção original das disposições remanescentes.

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

De acordo com a legislação vigente.

6. DOCUMENTOS REFERENCIADOS

6.1. Os documentos listados a seguir 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
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE PRESTADOR DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL	DOC-ICP-17
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02

[11]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05
[12]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP-12
[13]	POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06

6.2. Os documentos a seguir 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]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARS DA ICP-BRASIL	DOC-ICP-03.01
[9]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01
[10]	PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-BRASIL	DOC-ICP-05.02
[11]	REGULAMENTO DO USO DE BIOMETRIA NO ÂMBITO DA ICP BRASIL – SISTEMA BIOMÉTRICO DA ICPBRASIL	DOC-ICP-05.03
[12]	REQUISITOS ADICIONAIS PARA ADERÊNCIA AOS PROGRAMAS DE RAÍZES CONFIÁVEIS	DOC-ICP-01.02
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICA DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICPBRASIL	DOC-ICP-05

6.3. Os documentos a seguir são aprovados pela AC Raiz, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio http://www.iti.gov.br.

REF	NOME DO DOCUMENTO	CÓDIGO
[4]	MODELO DE TERMO DE TITULARIDADE	ADE-ICP-05.B

7. REFERÊNCIAS BIBLIOGRÁFICAS

[14] WebTrust Principles and Criteria for Registration Authorities, disponível em http://www.webtrust.org