



Declaração de Práticas de Negócio da AR CELEPAR

Edição: 10/01/2019

Versão 1.0

Sumário

- 1. INTRODUÇÃO 3
 - 1.1. VISÃO GERAL 3
 - 1.2. NOME DO DOCUMENTO DE PUBLICAÇÃO 3
 - 1.3. HIERARQUIA 3
 - 1.4. TIPOS DE CERTIFICADOS 3
 - 1.5. CONTATOS 4

- 2. PROCESSOS DE AUTORIDADE DE REGISTRO 4

- 3. IDENTIFICAÇÃO E AUTENTICAÇÃO 4
 - 3.1. ATRIBUIÇÃO DE NOMES 4
 - 3.1.1. TIPOS DE NOMES 4
 - 3.1.2. NECESSIDADE DOS NOMES SEREM SIGNIFICATIVOS 5
 - 3.2. VALIDAÇÃO INICIAL DA IDENTIDADE 5
 - 3.2.1. MÉTODO PARA COMPROVAR A POSSE DA CHAVE PRIVADA 5
 - 3.2.2. AUTENTICAÇÃO DA IDENTIFICAÇÃO DA ORGANIZAÇÃO 6
 - 3.2.2.1. DISPOSIÇÕES GERAIS 6
 - 3.2.2.2. DOCUMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UMA ORGANIZAÇÃO 6
 - 3.2.2.3. INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UMA ORGANIZAÇÃO 7
 - 3.2.3. AUTENTICAÇÃO DA IDENTIDADE DE UM INDIVÍDUO 7
 - 3.2.3.1. DOCUMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM INDIVÍDUO 7
 - 3.2.3.2. INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM INDIVÍDUO 8
 - 3.2.4. AUTENTICAÇÃO DA IDENTIDADE DE EQUIPAMENTO OU APLICAÇÃO 9
 - 3.2.4.1. PROCEDIMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM EQUIPAMENTO OU APLICAÇÃO 9
 - 3.2.4.2. INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM EQUIPAMENTO OU APLICAÇÃO 10
 - 3.2.5. PROCEDIMENTOS COMPLEMENTARES 10
 - 3.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES 10
 - 3.3.1. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA ROTINA DE NOVAS CHAVES ANTES DA EXPIRAÇÃO 10
 - 3.3.2. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA NOVAS CHAVES APÓS REVOGAÇÃO 11
 - 3.3.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO 11

- 4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO 11
 - 4.1. SOLICITAÇÃO DE CERTIFICADO 11
 - 4.1.1. QUEM PODE SUBMETER UMA SOLICITAÇÃO DE CERTIFICADO 12
 - 4.1.2. PROCESSO DE REGISTRO E RESPONSABILIDADES 12
 - 4.1.2.1. RESPONSABILIDADES DA AUTORIDADE DE REGISTRO 12
 - 4.1.2.2. OBRIGAÇÕES DAS AUTORIDADES DE REGISTRO 12
 - 4.2. PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO 13
 - 4.2.1. APROVAÇÃO OU REJEIÇÃO DE PEDIDOS DE CERTIFICADO 13
 - 4.2.2. TEMPO PARA PROCESSAR A SOLICITAÇÃO DE CERTIFICADO 13
 - 4.3. EMISSÃO DE CERTIFICADO 13
 - 4.4. ACEITAÇÃO DE CERTIFICADO 13
 - 4.5. USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO 13
 - 4.5.1. OBRIGAÇÕES DO TITULAR DO CERTIFICADO 13
 - 4.6. RENOVAÇÃO DE CERTIFICADOS 14
 - 4.7. REVOGAÇÃO DE CERTIFICADO 14
 - 4.7.1. CIRCUNSTÂNCIAS PARA REVOGAÇÃO 14
 - 4.7.2. QUEM PODE SOLICITAR A REVOGAÇÃO 14
 - 4.7.3. PROCEDIMENTO PARA SOLICITAÇÃO DE REVOGAÇÃO 15

- 5. DOCUMENTOS REFERENCIADOS 15

- 6. REFERÊNCIAS BIBLIOGRÁFICAS 16

CONTROLE DE ALTERAÇÕES

Responsável	Descrição / Alterações	Versão	Data
<i>Ivanise Cence Lopes</i>	<i>Versão inicial da DPN (modelo)</i>	<i>1.0</i>	<i>Dezembro/2019</i>

1. INTRODUÇÃO

O presente documento se aplica às entidades vinculadas à cadeia de certificação das Autoridades Certificadoras PRODEMGE, identificada como ACs PRODEMGE: AC PRODEMGE BR / AC PRODEMGE MG / AC PRODEMGE SSL / AC PRODEMGE CODESIGNING / AC PRODEMGE RFB.

1.1. VISÃO GERAL

Esta Divulgação das Práticas de Negócios (DPN) descreve as práticas e os procedimentos comerciais utilizados pela AR CELEPAR, vinculada operacionalmente às ACs PRODEMGE, integrantes da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Esta DPN está alinhada às Declarações de Práticas de Certificação (DPC), às Políticas de Certificado (PC) e à Política de Segurança (PS) das ACs PRODEMGE, e aos Princípios e Critérios WebTrust para AR (*WebTrust Principles and Criteria for Registration Authorities*).

A AR CELEPAR mantém todas as informações da sua DPN sempre atualizadas.

1.2. NOME DO DOCUMENTO DE PUBLICAÇÃO

Este documento é chamado “Declaração de Práticas de Negócio da AR CELEPAR”, referido a seguir simplesmente como “DPN” e descreve as práticas e os procedimentos comerciais empregados pela AR CELEPAR. Este documento é divulgado às ACs PRODEMGE.

1.3. HIERARQUIA

A AR CELEPAR está vinculada às Autoridades Certificadoras da Prodemge (ACs PRODEMGE), que estão vinculadas à AC PRODEMGE BR que por sua vez está vinculada hierarquicamente à Autoridade Certificadora Raiz Brasileira (AC Raiz).

1.4. TIPOS DE CERTIFICADOS

Com relação aos tipos específicos de certificados emitidos pela AR CELEPAR, devem ser observadas as Políticas de Certificado (PC) publicadas na página web <https://www.prodemge.gov.br/informacoes/politicas-e-praticas-de-certificacao>, que explicam como os certificados são gerados e administrados pelas ACs PRODEMGE e utilizados pela comunidade.

Políticas de Certificado	Nome conhecido	OID
Política de Certificado de Assinatura Digital tipo A1 da AC PRODEMGE MG	PC AC PRODEMGE MG A1	2.16.76.1.2.1.79
Política de Certificado de Assinatura Digital tipo A3 da AC PRODEMGE MG	PC AC PRODEMGE MG A3	2.16.76.1.2.3.90
Política de Certificado de Assinatura Digital tipo S1 da AC PRODEMGE MG	PC AC PRODEMGE MG S1	2.16.76.1.2.101.16
Política de Certificado de Assinatura Digital tipo S3 da AC PRODEMGE MG	PC AC PRODEMGE MG S3	2.16.76.1.2.103.14

Políticas de Certificado	Nome conhecido	OID
Política de Certificado de Assinatura Digital tipo A1 da AC PRODEMGE SSL	PC AC PRODEMGE SSL A1	2.16.76.1.2.1.95
Política de Certificado de Assinatura Digital tipo A1 da AC PRODEMGE CODESIGNING	PC AC PRODEMGE CODESIGNING A1	2.16.76.1.2.1.80
Política de Certificado de Assinatura Digital tipo A1 da AC PRODEMGE RFB	PC AC PRODEMGE RFB A1	2.16.76.1.2.1.23
Política de Certificado de Assinatura Digital tipo A3 da AC PRODEMGE RFB	PC AC PRODEMGE RFB A3	2.16.76.1.2.3.20
Política de Certificado de Assinatura Digital tipo A4 da AC PRODEMGE RFB	PC AC PRODEMGE RFB A4	2.16.76.1.2.4.7

1.5. CONTATOS

Nome da AR:	AR CELEPAR
Página Web:	http://www.celepar.pr.gov.br
Telefone:	(41) 3200-5000
Endereço:	Rua Mateus Leme, 1561, Bairro Bom Retiro – CEP 80520-174 - Curitiba - PR
E-mail:	celepar@celepar.pr.gov.br

2. PROCESSOS DE AUTORIDADE DE REGISTRO

A AR CELEPAR vinculada às ACs PRODEMGE, é responsável pelo processo de recebimento, validação e encaminhamento de solicitação de emissão ou revogação de certificados digitais e de identificação de seus solicitantes.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

A AR CELEPAR 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 direitos de propriedade intelectual de terceiros.

A AR CELEPAR reserva o direito, sem responsabilidade a qualquer solicitante, de rejeitar os pedidos.

3.1. ATRIBUIÇÃO DE NOMES

3.1.1. TIPOS DE NOMES

A AR valida certificados com nomes que possibilitam determinar a identidade da pessoa ou organização a que se referem.

O tipo de nome admitido para os titulares de certificados emitidos, segundo esta DPN, 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.

3.1.2. NECESSIDADE DOS NOMES SEREM SIGNIFICATIVOS

Os certificados emitidos pela AR 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.

3.2. VALIDAÇÃO INICIAL DA IDENTIDADE

Neste e nos itens seguintes estão descritos em detalhes os requisitos e procedimentos utilizados pela AR 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, cuja certidão original ou segunda via tenha sido emitida dentro dos 90 (noventa) dias anteriores à data da certificação. 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 referem-se 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 das ACs PRODEMGE.

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.

3.2.1. MÉTODO PARA COMPROVAR A POSSE DA CHAVE PRIVADA

A AR 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, os mesmos são descritos nessas PCs, no item correspondente.

3.2.2. AUTENTICAÇÃO DA IDENTIFICAÇÃO DA ORGANIZAÇÃO

3.2.2.1. DISPOSIÇÕES GERAIS

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

Em sendo o titular do certificado pessoa jurídica, é designada pessoa física como responsável pelo certificado, que será a detentora da chave privada. Preferencialmente, será designado como responsável pelo certificado o representante legal da pessoa jurídica ou um de seus representantes legais.

A confirmação da identidade é realizada mediante a presença física do interessado, com base em documentos de identificação legalmente aceitos e pelo processo de identificação biométrica da ICP-Brasil.

A AR realiza a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

- a) apresentação do rol de documentos elencados no item 3.2.2.2;
- b) apresentação do rol de documentos elencados no item 3.2.3.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado;
- c) presença física dos representantes legais, admitida a representação por procuração, conforme disposto no item 3.2, 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.

3.2.2.2. DOCUMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UMA ORGANIZAÇÃO

A confirmação da identidade de uma pessoa jurídica é feita pela AR mediante a apresentação de, no mínimo, os seguintes documentos:

- a) Relativos à sua habilitação jurídica:
 - i. Se pessoa jurídica criada ou autorizada por lei:
 1. Cópia do ato que a constituiu; e
 2. CNPJ;
 - ii. Se entidade privada:
 1. ato constitutivo, devidamente registrado no órgão competente; 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.

Preferencialmente, será designado como responsável pelo certificado o representante legal da pessoa jurídica ou um de seus representantes legais.

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.

3.2.2.3. INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UMA ORGANIZAÇÃO

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.

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 3.2.3.2.

3.2.3. AUTENTICAÇÃO DA IDENTIDADE DE UM INDIVÍDUO

A confirmação da identidade de um indivíduo é realizada mediante a presença física do interessado, com base em documentos de identificação legalmente aceitos e pelo processo biométrico da ICP-Brasil.

3.2.3.1. DOCUMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM INDIVÍDUO

Deverá ser apresentada a seguinte documentação, em sua versão original oficial, podendo ser física ou digital, por meio de barramento ou aplicação oficial, e coletada as seguintes biometrias para fins de identificação de um indivíduo solicitante de certificado:

- a) Registro de Identidade ou Passaporte, se brasileiro; ou
- b) Título de Eleitor, com foto; ou
- c) Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou
- 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[4]; e
- f) Impressões digitais do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03[4].

Nota 1: 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.

Nota 2: A AR reserva-se ao direito de somente aceitar a apresentação da Carteira de Trabalho e Previdência Social (CTPS) em complementação ao primeiro documento de identificação apresentado. A aceitabilidade da CTPS como documento único de identificação para emissão do Certificado Digital deverá passar por análise e parecer das ACs PRODEMGE.

Nota 3: Caso haja divergência dos dados constantes do documento de identidade, a emissão do certificado digital deverá ser suspensa e o solicitante orientado a regularizar sua situação junto ao órgão responsável.

Nota 4: Os documentos que possuem data de validade precisam estar dentro do prazo. Excepcionalmente, a CNH vencida poderá ser aceita para identificação de titular de certificado digital.

Nota 5: O e-mail de comunicação fornecido, deve ser exclusivo e obrigatório do titular do certificado digital, para garantia da integridade e segurança das informações prestadas.

Na hipótese de identificação positiva por meio do processo biométrico da ICP-Brasil fica dispensada a etapa de verificação de certificados da pessoa física. As evidências desse processo farão parte do dossiê eletrônico do requerente.

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 descrito no parágrafo a seguir dos documentos em papel.

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 a 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.

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.

3.2.3.2. INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM INDIVÍDUO

É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa física com as informações constantes nos documentos apresentados:

- a) Nome completo, sem abreviações; e
- b) Data de nascimento.

Cada PC pode definir como obrigatório o preenchimento de outros campos ou o titular do certificado poderá, a seu critério e mediante declaração expressa no Termo de Titularidade, solicitar o preenchimento de campos do certificado com as informações constantes nos seguintes documentos:

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

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 do Brasil, devendo a cópia da mesma ser arquivada junto à documentação, para fins de auditoria.

3.2.4. AUTENTICAÇÃO DA IDENTIDADE DE EQUIPAMENTO OU APLICAÇÃO

Se o titular for pessoa física, deverá ser feita a confirmação de sua identidade na forma do item 3.2.3.1 e esta assinará o termo de titularidade de que trata o item 4.1.

Se o titular for pessoa jurídica, deverá ser feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

- a) Apresentação do rol de documentos elencados no item 3.2.2.2;
- b) Apresentação do rol de documentos elencados no item 3.2.3.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado;
- c) Presença física do responsável pelo uso do certificado e assinatura do termo de titularidade e responsabilidade de que trata o item 4.1; e
- d) Presença física do(s) representante(s) legal(is) da pessoa jurídica e assinatura do termo de titularidade e responsabilidade de que trata o item 4.1, ou outorga de procuração atribuindo poderes para solicitação de certificado para equipamento ou aplicação e assinatura do respectivo termo de titularidade.

3.2.4.1. PROCEDIMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM EQUIPAMENTO OU APLICAÇÃO

Para certificados de equipamento ou aplicação que utilizem URL na identificação do titular, deve ser verificado se o solicitante do certificado detém o registro do nome de domínio junto ao órgão competente, ou se possui autorização do titular do domínio para usar aquele endereço. Nesse caso

deve ser apresentada documentação comprobatória (termo de autorização de uso de domínio ou similar) devidamente assinado pelo titular do domínio.

3.2.4.2. INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM EQUIPAMENTO OU APLICAÇÃO

É obrigatório o preenchimento dos seguintes campos do certificado com as informações constantes nos documentos apresentados:

- a) nome completo do responsável pelo certificado, sem abreviações;
- b) data de nascimento do responsável pelo certificado;
- c) nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, se o titular for pessoa jurídica;
- d) Cadastro Nacional de Pessoa Jurídica (CNPJ) se o titular for pessoa jurídica.

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 e responsabilidade, poderá solicitar o preenchimento de campos do certificado suas informações pessoais, conforme item 3.2.3.2.

3.2.5. PROCEDIMENTOS COMPLEMENTARES

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.

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].

3.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES

3.3.1. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA ROTINA DE NOVAS CHAVES ANTES DA EXPIRAÇÃO

Esta DPN estabelece os processos de identificação do solicitante utilizados pela AR vinculada às ACs PRODEMGE para a geração de novo par de chaves, e de seu correspondente certificado, antes da expiração de um certificado vigente.

Esse processo será conduzido conforme uma das seguintes possibilidades:

- a) adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado; ou

- 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.

3.3.2. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA NOVAS CHAVES APÓS REVOGAÇÃO

Após a revogação ou expiração do certificado, o solicitante pode solicitar um novo certificado, enviando à AR uma solicitação, na forma, condições e prazo estabelecidos para a solicitação inicial de um certificado.

3.3.3. 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 C PRODEMGE MG está descrito no item 4.7.3.

Solicitações de revogação de certificados devem ser registradas.

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1. SOLICITAÇÃO DE CERTIFICADO

Neste item são descritos todos os requisitos e procedimentos operacionais estabelecidos pela AR 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.

A solicitação de emissão de um Certificado Digital é feita mediante o preenchimento de formulário colocado à disposição do solicitante pela AR. Toda referência a formulário deverá ser entendida também como referência a outras formas que a AR possa vir a adotar. Dentre os requisitos e procedimentos operacionais estabelecidos pelas ACs para as solicitações de emissão de certificado, estão:

- 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 esfera estadual, 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[3] específico.

Nota 1: 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.

4.1.1. QUEM PODE SUBMETER UMA SOLICITAÇÃO DE CERTIFICADO

A submissão da solicitação deve ser sempre por intermédio da AR.

4.1.2. PROCESSO DE REGISTRO E RESPONSABILIDADES

Nos itens a seguir são descritas as obrigações gerais das entidades envolvidas. As obrigações específicas, quando aplicáveis, estão descritas nas PCs implementadas.

4.1.2.1. RESPONSABILIDADES DA AUTORIDADE DE REGISTRO

A AR será responsável pelos danos a que der causa.

4.1.2.2. OBRIGAÇÕES DAS AUTORIDADES DE REGISTRO

As obrigações da ARs 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 [2];
- 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 3.2.2, 3.2.3 e 3.2.7; 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 [2].

4.2. PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO

4.2.1. APROVAÇÃO OU REJEIÇÃO DE PEDIDOS DE CERTIFICADO

As ACs PRODEMGE e a AR CELEPAR podem, com a devida justificativa formal, aceitar ou rejeitar pedidos de certificados de requerentes de acordo com os procedimentos descritos nesta DPN.

4.2.2. TEMPO PARA PROCESSAR A SOLICITAÇÃO DE CERTIFICADO

As ACs PRODEMGE cumprem os procedimentos determinados na ICP-Brasil.

Não há tempo máximo para processar as solicitações na ICP-Brasil.

4.3. EMISSÃO DE CERTIFICADO

A emissão de certificado depende do correto preenchimento de formulário de solicitação, do recebimento do Termo de Titularidade, e dos demais documentos exigidos de acordo com as especificidades de cada tipo de certificado. Após o processo de validação das informações fornecidas pelo solicitante, o certificado é emitido.

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

4.4. ACEITAÇÃO DE CERTIFICADO

O titular do certificado ou pessoa física responsável verifica as informações contidas no certificado e o aceita caso as informações sejam íntegras, corretas e verdadeiras. Caso contrário, o titular do certificado não pode utilizar o certificado e deve solicitar imediatamente a revogação do mesmo. Ao aceitar o certificado, o titular do certificado:

- a) concorda com as responsabilidades, obrigações e deveres nesta DPN e na PC correspondente;
- b) garante que, com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada ao certificado;
- c) afirma que todas as informações contidas no certificado, fornecidas na solicitação, são verdadeiras e estão reproduzidas no certificado de forma correta e completa.

A aceitação de todo certificado emitido é declarada pelo respectivo titular. No caso de certificados emitidos para pessoas jurídicas, equipamentos ou aplicações, a declaração deverá ser feita pela pessoa física responsável por esses certificados.

Os certificados das ACs PRODEMGE são publicados de acordo com item 2.2 de suas DPCs.

4.5. USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO

4.5.1. OBRIGAÇÕES DO TITULAR DO CERTIFICADO

- a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
- b) garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;

- c) utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;
- d) conhecer os seus direitos e obrigações, contemplados pela DPC e pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil; e
- e) informar à AR CELEPAR qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

Nota: Em se tratando de certificado emitido para pessoa jurídica, estas obrigações se aplicam ao responsável pelo uso do certificado.

4.6. RENOVAÇÃO DE CERTIFICADOS

Em acordo com item 3.3 desta DPN.

4.7. REVOGAÇÃO DE CERTIFICADO

4.7.1. CIRCUNSTÂNCIAS PARA REVOGAÇÃO

O titular e o responsável pelo certificado podem solicitar a revogação de seu certificado a qualquer tempo, independente de qualquer circunstância.

O certificado deve ser obrigatoriamente revogado:

- a) Quando constatada emissão imprópria ou defeituosa do mesmo;
- b) Quando for necessária a alteração de qualquer informação constante no mesmo;
- c) No caso de dissolução de AC titular do certificado; ou
- d) No caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora.

As ACs PRODEMGE devem revogar, no prazo definido no item 4.9.3.3 de suas DPCs, o certificado do titular que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil.

Todo certificado tem a sua validade verificada, na respectiva LCR ou OCSP, antes de ser utilizado.

4.7.2. QUEM PODE SOLICITAR A REVOGAÇÃO

A revogação de um certificado somente pode ser feita:

- a) Por solicitação do titular do certificado;
- b) Por solicitação do responsável pelo certificado, no caso de certificado de equipamentos, aplicações e pessoas jurídicas;
- c) Por solicitação de empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;
- d) Pelas ACs PRODEMGE;
- e) Pela AR que tiver recebido a solicitação;

- f) Por determinação do CG da ICP-Brasil ou da AC Raiz; ou
- g) Por servidores públicos da ativa e militares da União, Estados e Distrito Federal autorizados pelos respectivos órgãos competentes pela identificação dos mesmos.

4.7.3. PROCEDIMENTO PARA SOLICITAÇÃO DE REVOGAÇÃO

Uma solicitação de revogação é necessária para que a AR responsável inicie o processo de revogação. O solicitante da revogação habilitado pode solicitar facilmente e a qualquer tempo a revogação de certificado, evitando assim a utilização indevida do certificado.

Instruções para a solicitação de revogação do certificado são obtidas no endereço <https://www.prodemge.gov.br/suporte/revogar> disponibilizada pelas ACs PRODEMGE.

A revogação é realizada através de Formulário on-line contendo o motivo da solicitação de revogação mediante o fornecimento de dados e da frase de identificação indicada na solicitação de emissão do Certificado.

Caso o Titular ou o Responsável - no caso de certificados de pessoas jurídicas ou aplicações - não recorde a frase de identificação ou quando a revogação é solicitada diretamente pelo Titular sem a participação do Responsável, o Formulário de revogação é impresso e assinado e entregue na AR CELEPAR.

O formulário disponível no site é preenchido com os dados do solicitante, o número de série do certificado e a indicação do motivo da solicitação.

Como diretrizes gerais:

- a) O solicitante da revogação de um certificado é identificado;
- b) As solicitações de revogação, bem como as ações delas decorrentes são registradas e armazenadas pelas ACs PRODEMGE;
- c) As justificativas para a revogação de um certificado são documentadas;
- d) O processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contém o certificado revogado e com a atualização da situação do certificado nas bases de dados das ACs PRODEMGE.

O prazo máximo admitido para a conclusão do processo de revogação de certificado de AC, após o recebimento da respectiva solicitação, é de 12 (doze) horas.

5. DOCUMENTOS REFERENCIADOS

Os documentos abaixo são encontrados no site oficial do ITI (<http://www.iti.gov.br>) e podem ser alterados, quando necessário, pelos órgãos competentes.

Ref.	Nome do documento	Código
[1]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-Brasil	DOC-ICP-03.01

[3]	TERMO DE TITULARIDADE	ADE-ICP-05. B
[4]	PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMÉTRICA NA ICP-Brasil	DOC-ICP-05.03
[5]	DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DAS ACs PRODEMGE	DPCs

6. REFERÊNCIAS BIBLIOGRÁFICAS

[2] PRINCÍPIOS E CRITÉRIOS WEBTRUST PARA AR (*WebTrust Principles and Criteria for Registration Authorities*), disponível em <http://www.webtrust.org>.