SOUZA MATOS CERTIFICACAO DIGITAL EIRELI
(AR ACERTE CERTIFICAÇÃO DIGITAL)
Vinculada à AC DIGITALSIGN e AC DIGITALSIGN RFB

DECLARAÇÕES DE PRÁTICAS DE NEGÓCIOS
VERSÃO 2.0 – 11/01/2023

HISTÓRICO DE VERSÕES

Data	*Versão*	*Observações*
02/04/2020	1.0	Redação Inicial
11/01/2023	2.0	Reformulação da DPN

CONTEÚDO

1. INTRODUÇÃO

1.1. VISÃO GERAL

1.1.1 Esta Declaração de Práticas de Certificação (DPC) descreve as práticas e os procedimentos utilizados pela Autoridade de Registro ACERTE CERTIFICAÇÃO DIGITAL, AR integrante na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) vinculada a AC Digitalsign.

A AR está certificada em nível imediatamente subsequente ao da Autoridade Certificadora Digitalsign, que por sua vez está vinculada a Autoridade Certificadora Principal da DigitalSign (AC DigitalSign ACP) certificada pela AC Raiz da ICP-Brasil.

Esta DPN, segue os mesmos procedimentos dos que os definidos nas ACs Digitalsign, disponível em:

https://www.digitalsigncertificadora.com.br/repositorio/media/files/Repositorio/AC/dpc_-_digitalsign.pdf

1.2. PARTICIPANTES DA ICP-BRASIL

1.2.1. Autoridades Certificadoras

O termo "Autoridade Certificadora" (AC) designa a entidade que emite e gere certificados digitais.

1.2.2. Autoridades de Registro

1.2.2.1. A Autoridade de Registo (AR) é uma entidade que desempenha o papel de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação dos seus solicitantes em nome da AC.

Esta DPN refere-se à Autoridade de Registro "AR ACERTE CERTIFICAÇÃO DIGITAL".

1.2.3. Titulares de Certificado

As pessoas físicas ou jurídicas de direito público ou privado, nacionais ou internacionais, que atendam aos requisitos da DPC e das PC da AC aplicáveis podem ser titulares de Certificado, para uso por pessoas físicas, pessoas jurídicas, em equipamentos ou aplicações.

1.2.4. 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. USABILIDADE DO CERTIFICADO

1.3.1. Uso Apropriado do Certificado

As descrições sobre o uso apropriado do certificado estão expressas na DPC da AC Digitalsign.

1.3.2. Uso Proibitivo do Certificado

Nas PC da AC DigitalSign e AC DigitalSign RFB correspondentes estão relacionadas, quando cabíveis, as aplicações para as quais existem restrições ou proibições para o uso desses certificados.

1.4. POLÍTICA DE ADMINISTRAÇÃO

1.4.1. Organização Administrativa do Documento

Nome: SOUZA MATOS CERTIFICACAO DIGITAL EIRELI

1.5 Procedimentos de Aprovação da DPC

Esta DPN é aprovada pela DigitalSign.

1.6. 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	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNH	Carteira Nacional de Habilitação
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
DETRAN	Departamento Nacional de Trânsito

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
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
PS	Política de Segurança
PSBio	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte

RFC	Request For Comments
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SIGEPE	SIGEPE Sistema de Gestão de Pessoal da Administração Pública Federal
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCSEC	Trusted System Evaluation Criteria
TLS	TLS Transport Layer Security
TSDM	Trusted Software Development Methodology
TSE	TSE Tribunal Superior Eleitoral
UF	Unidade de Federação
URL	URL Uniform Resource Locator

2. IDENTIFICAÇÃO E AUTENTICAÇÃO

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

2.1. VALIDAÇÃO INICIAL DE IDENTIDADE

Neste item e nos itens seguintes estão descritos em detalhe os requisitos e procedimentos utilizados pelas AR vinculadas à AC DigitalSign e AC DigitalSign RFB para a realização dos seguintes processos:

a) **Identificação do titular do certificado** – identificação da pessoa física ou jurídica, titular do certificado, com base nos documentos de identificação citados nos itens 2.1.2, 2.1.3 e 2.1.7, observado o quando segue:

i. para certificados de pessoa física: comprovação de que a pessoa física que se apresenta como titular do certificado é realmente aquela cujos dados constam na documentação e biometrias apresentadas, vedada qualquer espécie de procuração para tal fim.

ii. para certificados de pessoa jurídica: comprovação de que os documentos apresentados se referem efetivamente à pessoa jurídica titular do certificado e

de que a pessoa física que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição, admitida procuração por instrumento público, com poderes específicos para atuar perante a ICP-Brasil, cuja certidão original ou segunda via tenha sido emitida dentro de 90 (noventa) dias anteriores à data da solicitação.

iii. emissão do certificado: após a conferência dos dados da solicitação de certificado com os constantes dos documentos e biometrias apresentados, na etapa de identificação, é liberada a emissão do certificado no sistema da AC. 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.

2.1.1. Método para comprovar a Posse de 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. O descrito no RFC 4210, atualizada pela RFC 6712 é utilizado como referência para essa finalidade.

2.1.2. Autenticação da Identidade de uma Organização

2.1.2.1. Disposições Gerais

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

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

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

a) apresentação do rol de documentos elencados no item 2.1.3.1;

b) apresentação do rol de documentos elencados no item 2.1.2.2 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 2.1, alínea ‘a’, inciso (i) e do responsável pelo uso do certificado;

d) assinatura digital do termo de titularidade de que trata o item 3.1 pelo titular ou responsável pelo uso do certificado.

NOTA 01: Poderá a AC responsável e as AR a ela vinculada solicitar uma assinatura manuscrita ao titular ou responsável pelo uso do certificado para 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.

2.1.2.1.4. Fica dispensado o disposto no item 2.1.2.1.3., 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 2.1.2.2 possa ser realizada eletronicamente por meio de barramento ou aplicação oficial.

2.1.2.1.5. O disposto no item 2.1.2.1.3. poderá ser realizado:

a) mediante comparecimento presencial do responsável pelo certificado; ou

b) por videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz, os quais deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico.

2.1.2.2. 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 criada ou autorizada a sua criação por lei, cópia do CNPJ;
   ii. se entidade privada:
      1. certidão simplificada emitida pela Junta Comercial ou ato constitutivo, devidamente registrado no órgão competente, que permita a comprovação de quem são seus atuais representantes legais; e
      2. documentos da eleição de seus representantes legais, 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 01: Essas confirmações 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.

2.1.2.3 Informações contidas no certificado emitido para uma organização

2.1.2.3.1 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.

2.1.2.3.2 O modo como são preenchidos todos os campos estão presentes nas PC da AC DigitalSign e AC DigitalSign RFB.

2.1.2.4. Responsabilidade decorrente do uso do certificado de uma organização

Os atos praticados com o certificado digital de titularidade de uma organização estão sujeitos ao regime de responsabilidade definido em lei quanto aos poderes de representação conferidos ao responsável de uso indicado no certificado.

2.1.3. Autenticação da Identidade de um Indivíduo

Neste item devem ser definidos os procedimentos empregados pelas AR vinculadas a uma AC para a identificação e cadastramento iniciais de um indivíduo na ICP-Brasil. Essa confirmação deverá ser realizada mediante a presença física do interessado ou por um dos procedimentos listados nas alíneas abaixo, que deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico:

a) por módulo de AR eletrônico, exclusivamente nos casos previstos neste regulamento;
b) por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz; ou
c) por AR ELETRÔNICA, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz.

2.1.3.1. Procedimento para identificação de um indivíduo

A identificação da pessoa física requerente do certificado deverá ser realizada como segue:

a) apresentação da seguinte documentação, em sua versão original oficial, física ou digital:
    i. Registro de Identidade, se brasileiro; ou
    ii. Título de Eleitor, com foto; ou
    iii. Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou
    iv. Passaporte, se estrangeiro não domiciliado no Brasil.
b) coleta e verificação biométrica do requerente, conforme regulamentado em Instrução Normativa editada pela AC Raiz, a qual deverá definir os dados biométricos a serem coletados, bem como os procedimentos para coleta e identificação biométrica na ICP-Brasil.

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.

2.1.3.1.1 Na hipótese de identificação positiva por meio do processo biométrico da ICP-Brasil, ou por meio de processo de AR ELETRÔNICA, fica dispensada a apresentação de qualquer dos documentos elencados no item 2.1.3.1 e da etapa de verificação. As evidências desse processo farão parte do dossiê eletrônico do requerente.

2.1.3.1.2 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 2.1.3.1.3.

2.1.3.1.3 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 a etapa de identificação;

b) pela AR ou AR própria da AC ou ainda AR própria do PSS 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.

2.1.3.1.4 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.

2.1.3.2. Informações Contidas no Certificado Emitido para um Indivíduo

2.1.3.2.1. 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;

b) data de nascimento; e

c) Cadastro de Pessoa Física (CPF).

2.1.3.2.2. Cada PC da AC DigitalSign e AC DigitalSign 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, pode 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.

2.1.3.2.3. Para tanto, o titular deve apresentar a documentação respectiva, caso a caso, em 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 pode ser substituído por consulta à página da Receita Federal, devendo a cópia da mesma ser arquivada junto à documentação, para fins de auditoria.

2.1.4. Autenticação da Identidade de Equipamento ou Aplicação

2.1.4.1. DISPOSIÇÕES GERAIS

2.1.4.1.1. Tratando-se de certificado emitido para equipamento ou aplicação, o titular será a pessoa física ou jurídica solicitante do certificado, que deverá indicar o responsável pela chave privada.

2.1.4.1.2. Se o titular for pessoa física, deverá ser feita a confirmação da sua identidade na forma do item 2.1.3.1 e esta assinará o termo de titularidade de que trata o item 3.1.

2.1.4.1.3. Se o titular for pessoa jurídica, deverá ser feita a confirmação da identidade da organização e da pessoa física responsável pelo certificado, na forma do item 2.1.2

2.1.4.1.4. Fica dispensada a observância do disposto no item 2.2.3.1 para certificados cujo titular seja pessoa física, caso a solicitação seja assinada com certificado digital ICP-Brasil válido, do tipo A3 ou superior, de mesma titularidade e cujos dados biométricos já tenham sido devidamente coletados.

2.1.4.1.5. Fica dispensada a observância do item 2.1.2.1.3, alíneas "b" e "c", para certificados cujo titular seja pessoa jurídica nos seguintes casos:

a) quando a solicitação for assinada com certificado digital ICP-Brasil válido, do tipo A3 ou superior, de mesma titularidade e responsável, e cujos dados biométricos deste último tenham sido devidamente coletados; ou
b) quando a solicitação for assinada com o certificado digital ICP-Brasil válido, do tipo A3 ou superior, cuja titularidade é da mesma pessoa física responsável legal da organização e a verificação dos documentos elencados no item 2.1.2.2 possa ser realizada eletronicamente por meio de barramento ou aplicação oficial.

2.1.4.2. Procedimentos para Efeitos de Identificação de um Equipamento ou Aplicação

2.1.4.2.1. Para certificados de equipamento ou aplicação que utilizem URL no campo *Common Name*, 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 nome. Nesse caso deve ser apresentada documentação comprovativa (termo de autorização de uso de domínio ou similar) devidamente assinada pelo titular do domínio.

2.1.4.3. Informações Contidas no Certificado emitido para um equipamento ou aplicação

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

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

2.1.4.3.2. Cada PC da Digitalsign 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 suas informações pessoais, conforme item 2.1.3.2.2

2.1.5. Procedimentos Complementares

2.1.5.1 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.

2.1.5.2 Todo o processo de identificação do titular do certificado é 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. Tais registros são feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

2.1.5.3 É 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 em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil.

2.1.5.4 No caso de certificados emitidos em conjunto à Carteira de Identidade (RG) ou à Carteira Nacional de Habilitação (CNH), por Órgão de Identificação ou Departamento de Trânsito (Detran), dos Estados e do Distrito Federal, deverá ser mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade do indivíduo, incluindo, a Carteira de Identidade ou CNH emitida em conjunto ao certificado. Tais cópias poderão ser mantidas em papel ou em forma digitalizada, observadas as condições definidas em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil.

2.1.5.5. A ACs DigitalSigns 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 e DOC-ICP-05.02.

2.1.5.5.1 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 2.1.3.1.3.

2.2. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES

2.2.1. Identificação e Autenticação para rotina de Novas Chaves antes da Expiração

2.2.1.1. As DPCs da AC Digitalsign e AC DigitalSign RFB estabelece os processos de identificação do solicitante para a geração de novo par de chaves, e de seu correspondente certificado, antes da expiração do certificado vigente. O que por ela definido, esta DPN se subordina.

3. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

3.1. SOLICITAÇÃO DE CERTIFICADO

A solicitação de emissão de um Certificado Digital é feita mediante o preenchimento de formulário, seguindo os requisitos mínimos estabelecidos pela AC.

Dentre os requisitos e procedimentos operacionais estabelecidos pelas AC DigitalSign e AC DigitalSign RFB para as solicitações de emissão de certificado, estão:

a) a comprovação de atributos de identificação constantes do certificado, conforme item 2.2;

b) o uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes ao de um certificado de tipo A3 e a autenticação biométrica do agente de registro responsável pelas solicitações de emissão e de revogação de certificados; e

c) um termo de titularidade assinado digitalmente pelo titular do certificado ou pelo responsável pelo uso do certificado, no caso de pessoa jurídica, conforme o adendo referente ao TERMO DE TITULARIDADE 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.

3.1.1. Processo de Registro e Responsabilidades

Nos itens a seguir estão descritas as obrigações gerais das entidades envolvidas. Os requisitos específicos associados a essas obrigações estão detalhadas nas PC implementadas pelas AC DigitalSign e AC DigitalSign RFB, na qual esta AR está vinculada.

3.1.2.1. Responsabilidades da AC

3.1.2.1.1 A AC DigitalSign e AC DigitalSign RFB responde pelos danos a que der causa.

3.1.2.1.2 A DigitalSign responde solidariamente pelos atos das entidades de sua cadeia de certificação: AR e PSS.

3.1.2.2. Obrigações da AC

As obrigações das ACs geridas pela DigitalSign são:

a) operar de acordo com a DPC e com as PCs que implementa;

b) gerar e gerenciar seus pares de chaves criptográficas;

c) assegurar a proteção de suas chaves privadas;

d) notificar a AC Raiz, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação desse certificado;

e) notificar os usuários quando ocorrer suspeita de comprometimento da chave privada da AC DigitalSign, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;

f) distribuir seu próprio certificado;

g) emitir, expedir e distribuir os certificados de AR vinculadas e de usuários finais;

h) informar a emissão do certificado ao respectivo solicitante;

i) revogar os certificados emitidos;

j) emitir, gerenciar e publicar sua LCR e quando aplicável, disponibilizar consulta online de situação do certificado (*OCSP Online Certificate Status Protocol*);

k) publicar em sua página web sua DPC da AC DigitalSign e as PC que implementa;

l) publicar em sua página web as informações descritas no item 2.2.2 de sua DPC;

m) publicar em sua página web informações sobre o descredenciamento de AR;

n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;

o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;

p) adotar as medidas de segurança e controle previstas em sua DPC, PC e Política de Segurança que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;

q) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;

r) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;

s) manter e testar anualmente seu Plano de Continuidade do Negócio;

t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades;

u) informar à terceira parte e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pela AC;

v) informar à AC Raiz a quantidade de certificados digitais emitidos, conforme regulamentação da AC Raiz;

w) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;

x) realizar, ou delegar para seu PSS, as auditorias pré-operacionais e anualmente as auditorias operacionais de suas ARs, diretamente com seus profissionais, ou através de auditorias internas ou empresas de auditoria independente, ambas, credenciadas pela AC Raiz. O PSS deverá apresentar um único relatório de auditoria para cada AR vinculada às ACs que utilizam de seus serviços; e

y) garantir que todas as aprovações de solicitação de certificados sejam realizadas por agente de registro e estações de trabalho autorizados.

3.1.2.3. Responsabilidades da AR

A AR será responsável pelos danos a que der causa.

3.1.2.4. Obrigações das AR

As obrigações das AR vinculadas à AC DigitalSign são:

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 em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil;

d) informar os titulares de certificado 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 em regulamentos editados por instruções normativas da AC Raiz que definam os procedimentos operacionais para AR ELETRÔNICA e as características mínimas de segurança para as AR da ICP-Brasil, bem como os Princípios e Critérios WebTrust para AR;

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 desta DPN;

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.

3.2. PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO

3.2.1. Execução das funções de Identificação e Autenticação

A AC e AR executam as funções de identificação e autenticação conforme item 3 desta DPN.

3.2.2. Aprovação ou Rejeição de Pedidos de Certificado

3.2.2.1 A AC e AR podem, com a devida justificativa formal, aceitar ou rejeitar pedidos de certificados de requerentes de acordo com os procedimentos descritos nesta DPN e DPC da AC.

3.2.3. Tempo para Processar a Solicitação de Certificado

A AR cumpre os procedimentos determinados na ICP-Brasil. Não há tempo máximo para processar as solicitações na ICP-Brasil.

3.3. EMISSÃO DE CERTIFICADO

3.3.1. Ações da AC durante a emissão de um certificado

3.3.1.1. A emissão de certificado depende do correto preenchimento de formulário de solicitação, do recebimento do "Termo de Titularidade" no caso de certificados de pessoas jurídicas, equipamentos ou aplicações e dos demais documentos exigidos.

Após o processo de validação das informações fornecidas pelo solicitante, o certificado é emitido.

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

3.4. ACEITAÇÃO DE CERTIFICADO

3.4.1. Conduta sobre a Aceitação do Certificado

3.4.1.1. O titular do certificado ou pessoa física responsável verifica as informações contidas no certificado e aceita-o 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.

3.4.1.2. A aceitação do certificado e do seu conteúdo é declarada, pelo titular do certificado, pessoa física responsável no caso de o certificado ser emitido a pessoa jurídica, na primeira utilização da chave privada correspondente.

3.5. OBRIGAÇÕES DO TITULAR DO CERTIFICADO

As obrigações dos titulares de certificados emitidos pela AC DigitalSign, constantes dos termos de titularidade de que trata o item 3.1, são:

a) fornecer, de modo completo e preciso, todas as informações necessárias para a sua identificação;

b) garantir a proteção e o sigilo de suas chaves privadas, código de ativação (PIN) 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 da AC, pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil;

e) informar à AC DigitalSign o comprometimento ou suspeita de comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente; e

f) garantir a proteção do PUK, sendo permitido o gerenciamento por entidade autorizada pelo titular do certificado, mediante identificação presencial ou outro método com nível de segurança equivalente.

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

3.6. RENOVAÇÃO DE CERTIFICADOS

Em acordo com item 2.3 desta DPN.

3.6.1. Circunstâncias para Renovação de Certificados

Em acordo com item 2.3 desta DPN.

3.6.2. Quem Pode Solicitar a Renovação

Em acordo com item 2.3 desta DPN.

3.6.3. Processamento de Requisição para Renovação de Certificados

Em acordo com item 2.3 desta DPN.

3.6.4. Notificação para Nova Emissão de Certificado para o Titular

Em acordo com item 2.3 desta DPN.

3.6.5. Conduta constituindo a aceitação de uma Renovação de um Certificado

Em acordo com item 2.3 desta DPN.

3.7. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

3.7.1. Circunstâncias para Revogação

3.7.1.1. O titular do certificado e o responsável pelo certificado podem solicitar a revogação do seu certificado em qualquer altura e independentemente de qualquer circunstância.

3.7.1.2. O certificado é obrigatoriamente revogado:

a) quando for constatada emissão imprópria ou defeituosa do mesmo;

b) quando for necessária a alteração de qualquer informação constante no mesmo;

c) no caso de extinção, dissolução ou transformação da AC DigitalSign; ou

d) no caso de comprometimento ou suspeita de comprometimento da chave privada correspondente à pública contida no certificado ou da sua mídia armazenadora.

3.7.1.3. A AR ACERTE CERTIFICAÇÃO DIGITAL, solicita a revogação à AC Digitalsign que revoga, no prazo definido, o certificado do titular que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil.

O CG da ICP-Brasil ou AC Raiz determina a revogação do certificado da AC DigitalSign quando essa deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas pela ICP-Brasil.

3.7.2. Quem Pode Solicitar Revogação

A revogação de um certificado somente poderá 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) Pela AC DigitalSign;

e) Por uma AR vinculada;

f) Por determinação do CG da ICP-Brasil ou da AC Raiz;

3.7.3. Procedimento para Solicitação de Revogação

3.7.3.1. É necessária uma solicitação de revogação para que esta AR inicie o processo de revogação.

As instruções para a solicitação de revogação do Certificado são obtidas em página web disponibilizada pela AC DigitalSign ou por esta AR.

A revogação é realizada através de formulário contendo o motivo da solicitação de revogação e mediante o fornecimento de dados indicados na solicitação de emissão do certificado, ou por formulário assinado pelo titular na falta desses dados.

3.7.3.2. Como diretrizes gerais:

a) O Solicitante da revogação de um certificado é identificado;

b) As solicitações de revogação, bem como as ações delas decorrentes serão registradas e armazenadas pela AC DigitalSign;

c) As justificativas para a revogação de um certificado são registradas;

d) O processo final de revogação de um certificado termina com a geração e a publicação da LCR que contenha o certificado revogado e com a atualização do estado do certificado em resposta OCSP à base de dados da AC DigitalSign, quando aplicável.

3.7.3.3. O prazo máximo para conclusão do processo de revogação do certificado pela AC DigitalSign, após a conclusão do processo de aceitação e registro da solicitação de revogação é de 24 (doze) horas.

3.7.4. Prazo para Solicitação de Revogação

3.7.4.1. O prazo para aceitação do certificado pelo seu titular é de 3 (três) dias, dentro do qual a revogação desse certificado pode ser solicitada sem cobrança de tarifa de revogação.

3.8. ENCERRAMENTO DE ATIVIDADES

3.8.1 Em caso de extinção da AR serão tomadas as providências preconizadas no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL.

4. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

4.1. TARIFAS

4.1.1. Tarifas de Emissão e Renovação de Certificados

Pela emissão e renovação do certificado será cobrado o valor estabelecido contratualmente.

4.1.2. Tarifas de Acesso ao Certificado

Não são cobradas tarifas de acesso ao certificado digital emitido.

4.1.3. Tarifas de Revogação ou de Acesso à Informação de Status

Pela revogação ou acesso à informação de status do certificado será cobrado o valor estabelecido contratualmente.

4.1.4. Tarifas para Outros Serviços

Pelos demais serviços será cobrado o valor estabelecido contratualmente.

4.1.5. Política de Reembolso

Em caso de revogação do certificado por motivo de comprometimento da chave privada ou da mídia armazenadora da chave privada da AC DigitalSign, ou ainda quando constatada a emissão imprópria ou defeituosa imputável à AR ACERTE CERTIFICAÇÃO DIGITAL ou AC DigitalSign, será emitido gratuitamente outro certificado em substituição.

4.2. CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO

4.2.1. Escopo de Informações Confidenciais

4.2.1.1. Como princípio geral, todos os documentos, informações ou registros fornecidos à AC ou às AR são sigilosos.

4.2.1.2. Nenhum documento, informação ou registro fornecido pelos titulares de certificado à AR responsável por esta DPN será divulgado.

4.2.2. Informações fora do escopo de Informações Confidenciais

Não são consideradas informações sigilosas:

a) os certificados e LCR/OCSP emitidos pela AC DigitalSign;

b) informações corporativas ou pessoais que constem nos certificados ou em diretórios públicos;

c) as PC implementadas pela AC;

d) a DPC da AC;

e) versões públicas de Políticas de Segurança da AC;

f) resultados finais de auditorias;

g) esta DPN.

4.2.3. Responsabilidade em proteger a Informação Confidencial

4.2.3.1. Os participantes que receberem ou tiverem acesso a informações confidenciais devem possuir mecanismos para assegurar a proteção e a confidencialidade, evitando o seu uso ou divulgação a terceiros, sob pena de responsabilização, na forma da lei.

4.2.3.2. Os titulares (ou os responsáveis no caso de pessoa jurídica) dos certificados de assinatura emitidos são responsáveis pela geração, manutenção e sigilo de suas respectivas chaves privadas, bem como pela divulgação ou utilização indevida dessas mesmas chaves.

4.3. LIMITAÇÕES DE RESPONSABILIDADES

A AR responsável por esta DPN não responde pelos danos que não lhe sejam imputáveis ou a que não tenha dado causa, na forma da legislação vigente.

4.4. INDENIZAÇÕES

A AR responsável por esta DPN responde pelos danos que der causa, e lhe sejam imputáveis, na forma da legislação vigente, assegurado o direito de regresso contra o agente ou entidade responsável.

4.5. PRAZO E RESCISÃO

4.5.1. Prazo

Esta DPN entra em vigor a partir da publicação que a aprovar, e permanecerá válida e eficaz até que venha a ser revogada ou substituída, expressa ou tacitamente.

4.5.2. Término

Esta DPN vigorará por prazo indeterminado, permanecendo válida e eficaz até que venha a ser revogada ou substituída, expressa ou tacitamente.

4.5.3. EFEITO DA RESCISÃO E SOBREVIVÊNCIA

Os atos praticados na vigência desta DPN são válidos e eficazes para todos os fins de direito, produzindo efeitos mesmo após a sua revogação ou substituição.

4.6. AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES

As notificações, intimações, solicitações ou qualquer outra comunicação necessária sujeita às práticas descritas nesta DPN serão feitas, preferencialmente, por e-mail assinado digitalmente, ou, na sua impossibilidade, por escrito e entregue à AC DigitalSign.

4.7. SOLUÇÃO DE CONFLITOS

4.7.1. Os litígios decorrentes desta DPN serão solucionados de acordo com a legislação vigente.

4.8. LEI APLICÁVEL

Esta DPN é regida pela legislação da República Federativa do Brasil, notadamente a Medida Provisória Nº 2.200-2, de 24.08.2001, e a legislação que a substituir ou alterar, bem como pelas demais leis e normas em vigor no Brasil.

4.9. CONFORMIDADE COM A LEI APLICÁVEL

A AR responsável por esta DPN está sujeita à legislação que lhe é aplicável, comprometendo-se a cumprir e a observar as obrigações e direitos previstos em lei.

4.10. DISPOSIÇÕES DIVERSAS

4.10.1. Acordo Completo

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

4.10.2. Cessão

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

4.10.3. Independência de Disposições

A invalidade, nulidade ou ineficácia de qualquer das disposições desta DPN 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 DPN será interpretada como se não contivesse tal disposição, e na medida do possível, mantendo a intenção original das disposições remanescentes.

4.10.4. Execução (Honorários dos Advogados e Renúncia de Direitos)

De acordo com a legislação vigente.

5. REFERÊNCIAS BIBLIOGRÁFICAS

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

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. 11.515/NB 1334: Critérios de segurança física relativos ao armazenamento de dados. 2007.

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

RFC 4210, IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), september 2005.

RFC 5019, IETF - The Lightweight Online Certificate Status Protocol (OCSP) Profile for HighVolume Environments, september 2007

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

RFC 6712, IETF - Internet X.509 Public Key Infrastructure - HTTP Transfer for the Certificate Management Protocol (CMP), september 2012.

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