



DISPOSITIVO AUTORIZADOR FISCAL

Especificação Técnica de Requisitos

Revisão: 1.0.0

30 de junho de 2021

Instituto Federal de Santa Catarina

Coordenação

Emerson Ribeiro de Mello, Dr.

Roberto de Matos, Dr.

Corpo técnico

Jaqueline Rissá Franco, Ma.

Paulo Fylippe Sell

Rafael Gustavo Nagel

Sarom Torres

Yan Lucas Martins

Secretaria de Estado da Fazenda de Santa Catarina

Coordenação

Rogério de Mello Macedo da Silva

Sérgio Dias Pinetti

Participantes

Clóvis Luis Jacoski

Cristiano Fornari Colpani

Edson Gonzaga Polonini

Édwin Floriani

Erich Rizza Ferraz

Felipe Letsch

Luiz Carlos Jung

Paulo Roberto Barros Gotelipe

Thiago Rocha Chaves

Copyright © 2020-2021 Secretaria de Estado da Fazenda de Santa Catarina.
Todos direitos reservados e protegidos pela Lei 9.610 de 19/02/1998.

Histórico de revisões

Revisão	Data	Descrição
1.0.0	30.06.2021	Versão inicial

Sumário

Sumário	3
Siglas	8
Glossário	10
Lista de Figuras	13
Lista de Tabelas	14
Lista de Códigos	17
Lista de Algoritmos	19
1 Introdução	20
1.1 Terminologia para indicar os níveis de exigência	22
2 Visão geral do DAF	23
2.1 Artefatos	24
2.2 Estados de operação	25
2.3 Arquitetura de memória	28
2.4 Requisitos da arquitetura do DAF	29
2.4.1 Requisitos criptográficos	29
2.4.2 Requisitos do identificador único do DAF	30
2.4.3 Requisitos da memória imutável	31
2.4.4 Requisitos da memória mutável	31
2.4.5 Requisitos da memória protegida	32
2.4.6 Requisitos do <i>bootloader</i>	32
2.4.7 Requisitos do modo inutilizado	33
2.4.8 Requisitos do <i>software</i> básico	34
2.4.9 Requisitos para atualização do SB	34
3 Organização do DAF	35
3.1 Microcontrolador seguro	35
3.2 Memória externa não volátil	36
3.3 Organização das memórias	36
3.4 Alimentação	36
3.5 Gabinete e sistema anti-fuligem	36

3.6	Interface de comunicação	37
3.7	Sinalização	38
4	Software Básico	39
4.1	Cenários de uso	39
4.2	Descrição dos casos de uso do DAF	40
4.3	Classificação dos casos de uso	51
5	Processos operacionais com o DAF	52
5.1	Registro do DAF junto à SEF	52
5.1.1	Exceções	54
5.2	Autorização de Documentos Fiscais Eletrônicos (DF-e)	56
5.2.1	Conjunto de informações essenciais do DF-e a ser montado pelo PAF	58
5.2.2	Representação da autorização gerada pelo DAF	58
5.2.3	Incorporação da autorização gerada pelo DAF nos DF-e	59
5.2.4	Autorização de DF-e diante de rejeições da SEFAZ autorizadora	59
5.2.5	Exceções	59
5.3	Apagar autorizações retidas no DAF	61
5.3.1	Exceções	62
5.4	Apagar autorizações retidas no DAF sobre DF-e com rejeição	62
5.5	Remover registro do DAF junto à SEF	64
5.5.1	Exceções	66
5.6	Atualizar Software Básico	67
5.6.1	Exceções	68
5.7	Atualizar certificado digital SEF	70
5.7.1	Exceções	71
5.8	Alterar modo de operação do DAF	71
5.8.1	Exceções	73
6	Protocolo de comunicação	75
6.1	API DAF	75
6.1.1	Representação dos pedidos e respostas da API DAF	75
6.1.2	Pedidos e respostas da API DAF	77
6.2	Protocolo DAF-USB	86
6.2.1	Formato do quadro do PDAF-USB	87
6.2.2	Garantia de entrega	88
6.2.3	Enquadramento	89
6.2.4	Detalhamento dos comandos e confirmação do PDAF-USB	90
7	Serviços providos pela SEF	92
7.1	Processos operacionais para fabricantes de DAF	92
7.1.1	Iniciar registro de modelo de DAF	93
7.1.2	Concluir registro de modelo de DAF	94
7.1.3	Revogar pedido de registro de modelo de DAF	94
7.1.4	Publicar <i>software</i> básico	94
7.2	Processos operacionais para entidades certificadoras de DAF	95

7.3	Processos operacionais para desenvolvedores de PAF	95
7.3.1	Registrar PAF	95
7.3.2	Remover registro de PAF	95
7.3.3	Publicar idPAF de contribuinte	95
7.3.4	Excluir idPAF de contribuinte	96
7.4	Processos operacionais para auditores fiscais da SEF	96
7.4.1	Verificar informações do DAF	96
7.5	Processos operacionais para o Fisco	96
7.5.1	Revogar modelo de DAF	96
7.5.2	Revogar PAF	96
7.5.3	Suspender uso de DAF	96
7.6	Processos operacionais para o PAF	97
7.6.1	Registrar DAF	97
7.6.2	Remover registro de DAF	97
7.6.3	Atualizar <i>software</i> básico	97
7.6.4	Consultar situação DAF	98
7.6.5	Recuperar chave PAF	98
7.6.6	Informar extravio de DAF	98
7.6.7	Atualizar certificado SEF	98
7.6.8	Alterar modo de operação do DAF	98
7.6.9	Obter resultado sobre autorização de DF-e	99
7.6.10	Solicitar resultado sobre autorização de DF-e com rejeição	99
7.6.11	Solicitar remoção extraordinária de autorização retida	100
8	Interfaces dos Serviços <i>Web</i>	101
8.1	Padrões técnicos	102
8.1.1	Padrão de comunicação	102
8.1.2	Padrão de assinatura digital	103
8.2	Padrão de mensagens XML	104
8.3	Representação de tokens JWT	105
8.4	Regras de validação dos Serviços <i>Web</i>	105
8.4.1	Regras gerais de validação	105
8.4.2	Regras específicas de negócio	105
8.5	Serviço <i>Web</i> - DAFRegistroDispositivo	107
8.5.1	iniciarRegistro	107
8.5.2	confirmarRegistro	108
8.6	Serviço <i>Web</i> - DAFRemocaoRegistro	111
8.6.1	removerRegistro	111
8.6.2	confirmarRemoverRegistro	112
8.7	Serviço <i>Web</i> - DAFResultadoAutorizacao	114
8.7.1	obterResultadoAutorizacao	114
8.8	Serviço <i>Web</i> - DAFAutorizacaoRetida	116
8.8.1	encaminharDFeRejeitado	117
8.8.2	encaminharAutorizacoesRetidas	118
8.8.3	consultarAutorizacaoApagar	120

8.9	Serviço <i>Web</i> - DAFavisoExtravio	122
8.9.1	avisarExtravio	122
8.10	Serviço <i>Web</i> - DAFAlteracaoModoOperacao	123
8.10.1	alterarModoOperacao	123
8.10.2	confirmarModoOperacao	125
8.11	Serviço <i>Web</i> - DAFConsultaSB	127
8.11.1	consultarVersaoSB	127
8.12	Serviço <i>Web</i> - DAFAtualizacaoCertificado	129
8.12.1	solicitarCertificado	129
8.13	Serviço <i>Web</i> - DAFConsultaDispositivo	130
8.13.1	consultarDispositivo	130
8.14	Serviço <i>Web</i> - DAFSolicitacaoChavePAF	132
8.14.1	solicitarChavePAF	132
Referências		134
Apêndices		136
A	Exemplos de como representar documentos JSON das mensagens da API do DAF	137
A.1	Pedidos sem assinatura digital	137
A.2	Respostas sem assinatura digital	138
A.3	Pedidos com assinatura digital	139
A.4	Respostas com assinatura digital	139
A.5	Como representar chave pública RSA no <i>Header</i> de um <i>token</i> JWT	140
A.6	Como representar chave pública EC no <i>Header</i> de um <i>token</i> JWT	140
A.7	Como representar a chave SEF cifrada utilizando <i>token</i> JWE	140
B	Exemplos de mensagens por processo operacional com o DAF	142
B.1	Registro do DAF junto à SEF	142
B.1.1	Mensagem DAF consultarInformacoes	142
B.1.2	Serviço SEF DAFRegistroDispositivo - método iniciarRegistro	143
B.1.3	Mensagem DAF registrar	144
B.1.4	Serviço SEF DAFRegistroDispositivo - método confirmarRegistro	147
B.1.5	Mensagem DAF confirmarRegistro	149
B.2	Remover registro do DAF junto à SEF	149
B.2.1	Serviço SEF DAFRemocaoRegistro - método removerRegistro	150
B.2.2	Mensagem DAF removerRegistro	151
B.2.3	Serviço SEF DAFRemocaoRegistro - método confirmarRemoverRegistro	152
B.2.4	Mensagem DAF confirmarRemocaoRegistro	153
B.3	Autorização de Documentos Fiscais Eletrônicos (DF-e)	153
B.3.1	Mensagem DAF solicitarAutenticacao	153
B.3.2	Mensagem DAF autorizarDFE	154
B.4	Apagar autorizações retidas no DAF	156
B.4.1	Serviço SEF DAFResultadoAutorizacao - método obterResultadoAutorizacao	156
B.4.2	Mensagem DAF apagarAutorizacaoRetida	157
B.5	Solicitar remoção extraordinária de autorizações retidas no DAF	157

B.5.1	Mensagem DAF consultarInformacoes	157
B.5.2	Mensagem DAF descarregarRetido	158
B.5.3	Serviço DAFAutorizacaoRetida - método encaminharAutorizacoesRetidas	159
B.5.4	Serviço SEF DAFAutorizacaoRetida - método consultarAutorizacaoApagar	160
B.5.5	Mensagem DAF apagarAutorizacaoRetida	161

C Pseudocódigos para representação das máquinas de estado do PDAF-CDC 162

Siglas

AC Autoridade Certificadora (*Veja: [Autoridade Certificadora](#)*).

ACM *Abstract Control Model*.

API *Application Programming Interface* (*Veja: [Application Programming Interface](#)*).

BP-e Bilhete de Passagem Eletrônico.

CNPJ Cadastro Nacional da Pessoa Jurídica.

CSR *Certificate Signing Request* (*Veja: [Certificate Signing Request](#)*).

CSRT Código de Segurança do Responsável Técnico (*Veja: [Código de Segurança do Responsável Técnico](#)*).

DAF Dispositivo Autorizador Fiscal.

DF-e Documento Fiscal Eletrônico.

EC *Elliptic Curve*.

ECDH *Elliptic-curve Diffie–Hellman*.

ECIES *Elliptic Curve Integrated Encryption Scheme*.

GESAC Grupo Especialista Setorial em Automação Comercial da Secretaria de Estado da Fazenda de Santa Catarina (SEF).

HMAC *Hash-based Message Authentication Code* (*Veja: [Hash-based Message Authentication Code](#)*).

IdAut Identificador único da autorização DAF (*Veja: [Identificador único da autorização DAF](#)*).

IdDAF Identificador único do DAF (*Veja: [Identificador único do DAF](#)*).

IdPAF Identificador único do PAF (*Veja: [Identificador único do PAF](#)*).

IdPDV Identificador único do [Ponto de Venda](#) (PDV).

JSON *JavaScript Object Notation*.

JWA *JSON Web Algorithms*.

JWE *JSON Web Encryption*.

JWK *JSON Web Key*.

JWT *JSON Web Token*.

LED Diodo Emissor de Luz.

MGF1 *Mask Generation Function 1*.

MT Memória de Trabalho (*Veja: Memória de Trabalho*).

NFC-e Nota Fiscal de Consumidor Eletrônica.

PAF Programa Aplicativo Fiscal.

PDAF-USB Protocolo DAF-USB.

PDV Ponto de Venda (*Veja: Ponto de Venda*).

PEM *Privacy Enhanced Mail*).

PKCS *Public Key Cryptography Standards*.

RAM *Random-access memory*.

RFC *Request for Comments*.

ROM *Read-only memory*.

RSA Rivest-Shamir-Adleman.

SB *Software Básico* (*Veja: Software Básico*).

SBC *Software Básico Candidato* (*Veja: Software Básico Candidato*).

SEF Secretaria de Estado da Fazenda de Santa Catarina.

SEFAZ Secretaria de Estado da Fazenda.

SINIEF Sistema Nacional Integrado de Informações Econômico - Fiscais.

SOAP *Simple Object Access Protocol*.

SVRS [SEFAZ Virtual do Rio Grande do Sul](#).

TLS *Transport Layer Security*.

TRNG *True Random Number Generator* (*Veja: True Random Number Generator*).

UML *Unified Modeling Language*.

URL *Uniform Resource Locator*.

USB *Universal Serial Bus*.

USB-CDC *USB Communication Device Class*.

UUID *Universally Unique Identifier* (*Veja: Universally Unique Identifier*).

W3C *World Wide Web Consortium*.

WS-I BP *Web Services Interoperability Basic Profile*.

XML *eXtensible Markup Language*.

Glossário

Application Programming Interface conjunto de regras e especificações que um software deve seguir para conseguir acessar e fazer uso de recursos e serviços ofertados por um software que implementa essa API.

Assinatura digital assinatura digital é um mecanismo capaz de garantir que uma mensagem foi criada por uma determinada entidade, bem como capaz de afirmar que o conteúdo da mensagem não foi alterado.

Autoridade Certificadora responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Na emissão de certificados tem a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Desta forma, o certificado emitido pela AC representa a declaração da identidade do titular, o qual possui o par único de chaves (pública/privada).

Bootloader O *bootloader* do [Dispositivo Autorizador Fiscal \(DAF\)](#), denominado apenas de *bootloader* ao longo deste documento, reúne o sistema básico executado após o processo de inicialização do microcontrolador. O *bootloader* do [DAF](#) pode coexistir com um *bootloader* embutido de fábrica da [Read-only memory \(ROM\)](#). Neste caso, o *bootloader* do [DAF](#) assume a execução do processador imediatamente após a execução do *bootloader* da [ROM](#).

Certificado digital da SEF certificado digital da [Secretaria de Estado da Fazenda de Santa Catarina \(SEF\)](#) incluído na memória segura do dispositivo em tempo de manufatura. Deverá ser usado pelo *bootloader* e pelas rotinas internas do [Software Básico \(SB\)](#).

Certificate Signing Request solicitação de assinatura de certificado é uma mensagem enviada por uma entidade a uma [Autoridade Certificadora \(AC\)](#) para solicitar um certificado de identidade digital.

Chave de ateste chave privada incluída na memória segura do dispositivo em tempo de manufatura. Essa chave é usada durante o processo de registro do [DAF](#) junto à [SEF](#). A chave de ateste deverá ser única para cada modelo de [DAF](#).

Chave PAF número arbitrário gerado pela [SEF](#) e único para cada [Programa Aplicativo Fiscal \(PAF\)](#), após processo de registro do [DAF](#).

Chave privada chave criptográfica utilizada em um algoritmo de criptografia assimétrica e associada a uma chave pública. Esta chave é associada com um emissor e não deve ser compartilhada. Pode ser utilizada para assinar mensagens que posteriormente serão verificadas com a [chave pública](#) correspondente.

Chave privada do DAF chave privada gerada pela rotina de registro do **DAF** junto à **SEF**.

Chave pública chave criptográfica utilizada em um algoritmo de criptografia assimétrica e associada a uma chave privada. Esta chave é associada com um emissor e pode ser compartilhada. Quando utilizada em assinaturas digitais, é utilizada para verificar se a mensagem foi assinada pela **chave privada** correspondente.

Chave SEF número arbitrário gerado pela **SEF** e único para cada **DAF**, após processo de registro do **DAF**.

Código de Segurança do Responsável Técnico código de segurança alfanumérico (16 a 36 *bytes*) de conhecimento apenas da Secretaria da Fazenda da Unidade Federada do emitente e da empresa responsável pelo sistema emissor de **Documento Fiscal Eletrônico (DF-e)**.

Contador monotônico contador que incrementa de forma monotônica a cada operação de autorização sobre **DF-e** realizada pelo **DAF**.

Contribuinte pessoa física ou jurídica que paga tributo aos cofres públicos do Estado.

E-CNPJ certificado digital e-CNPJ é um documento eletrônico de identidade emitido por **AC** credenciada pela Autoridade Certificadora Raiz da **ICP-Brasil** (**AC Raiz**) e habilitada pela Autoridade Certificadora da Receita Federal Brasileira (**AC-RFB**), que certifica a autenticidade dos emissores e destinatários dos documentos e dados que trafegam numa rede de comunicação, bem assim assegura a privacidade e a inviolabilidade destes.

Firmware *software* embarcado desenvolvido especificamente para o *hardware* onde está implantado.

Função hash criptográfica função criptográfica que recebe uma entrada de comprimento variável e gera uma saída de comprimento fixo, sendo essa chamada de resumo criptográfico ou *hash*. A função é de sentido único, ou seja, a partir da saída não é possível obter a entrada original.

Hash-based Message Authentication Code código de autenticação com base em **resumo criptográfico** que é gerado a partir de uma chave criptográfica secreta e uma **função hash criptográfica**.

ICP-Brasil infraestrutura de chave pública Brasileira é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais.

IdCSRT identificador do **Código de Segurança do Responsável Técnico (CSRT)** utilizado para geração do **Identificador único do PAF (IdPAF)**.

Identificador único da autorização DAF código de identificação único de cada autorização realizada pelo **DAF**. Esse código consiste na saída, representada em Base64URL, de uma **função hash criptográfica HMAC-SHA256** que teve como chave a **chave SEF** e como mensagem o valor de seu **contador monotônico** no momento da autorização, o fragmento XML com as informações essenciais do **DF-e** e o **resumo criptográfico** sobre o XML completo do **DF-e** em questão.

Identificador único do DAF número único por dispositivo incluído na memória segura do dispositivo em tempo de manufatura. Esse identificador deve ser um *Universally Unique Identifier (UUID)*.

Identificador único do PAF código de identificação único do **PAF** por contribuinte. Esse código consiste na saída, codificada em Base64URL, de uma **função hash criptográfica HMAC-SHA256**, tendo o **CSRT** do desenvolvedor do **PAF** como chave e o **CNPJ** do **contribuinte** como mensagem.

Memória de Trabalho conjunto de recursos em *hardware* destinado à gravação de dados para apoio do funcionamento do *Software Básico (SB)*.

Modo de operação do DAF indica se o DAF é operado por apenas um PDV ou compartilhado por mais de um PDV.

Modo inutilizado conjunto de rotinas que implementam as funcionalidades do estado INUTILIZADO.

Nonce palavra de uso único empregada em processos criptográficos, por exemplo, em protocolos de autenticação para evitar ataque de repetição. A palavra pode ser uma sequência de símbolos gerada de forma aleatória.

Partição de atualização região de memória reservada para armazenar o *Software Básico Candidato (SBC)* durante o processo de atualização segura.

Ponto de Venda local onde cliente e comerciante concretizam uma operação comercial. Consiste na combinação de *hardware*, como caixa registradora, balança, etc, e *software*, como *sistema de automação comercial* e sistema para emissão de documentos fiscais.

Resumo criptográfico resumo criptográfico ou *hash* criptográfico é a saída de uma *função hash* criptográfica.

Rotinas criptográficas conjunto de rotinas para gerar pares de chaves criptográficas, para gerar e verificar assinaturas e *resumos criptográficos*.

Sistema de automação comercial sistema responsável para automatizar processos como controle de estoque, cadastro de produtos, cadastro de clientes e fornecedores, etc.

Software Básico conjunto de rotinas, residentes no DAF que implementa as funções de controle fiscal.

Software Básico Candidato imagem contendo a nova versão *Software Básico (SB)* a ser instalada no DAF.

Transação atômica conjunto de operações que deve ser executado em sua totalidade em caso de sucesso. Deve ser abortado por completo em caso de erro, fazendo com que retorne para o estado anterior ao início da execução da transação.

True Random Number Generator componente físico que gera uma sequência de símbolos aleatórios que não pode ser prevista.

Universally Unique Identifier identificador único universal consiste de um número de 128 *bits* que será usado para identificar de forma inequívoca cada DAF.

Lista de Figuras

1.1	Entidades do projeto DAF	21
1.2	Diagrama de implantação com o PAF no modelo cliente e servidor	21
2.1	Visão geral da arquitetura do DAF.	23
2.2	Máquina de estados do Dispositivo Autorizador Fiscal	26
2.3	Fluxograma do comportamento do <i>bootloader</i>	32
3.1	Organização do DAF com os componentes e interligações	35
4.1	Diagrama de caso de uso do DAF	39
5.1	Diagrama de sequência do processo de registro do DAF	53
5.2	Diagrama de atividade do processo de registro do DAF	55
5.3	Diagrama de sequência do processo de autorização de um DF-e	56
5.4	Diagrama de atividade do processo de autorização de um DF-e	60
5.5	Diagrama de sequência do processo para apagar autorizações retidas	61
5.6	Diagrama de atividade do processo para apagar autorizações retidas	62
5.7	Diagrama de sequência do processo para apagar autorizações retidas, de documentos com rejeições	63
5.8	Diagrama de sequência do processo para remover o registro do DAF junto à SEF	64
5.9	Diagrama de atividade do processo para remover o registro do DAF junto à SEF	66
5.10	Diagrama de sequência do processo para atualizar o SB do DAF	67
5.11	Diagrama de atividade do processo para atualizar o SB do DAF	69
5.12	Diagrama de sequência do processo para atualizar o certificado digital SEF no DAF	70
5.13	Diagrama de atividade do processo para atualizar o certificado digital SEF no DAF	71
5.14	Diagrama de sequência do processo para alterar o modo de operação do DAF	72
5.15	Diagrama de atividade do processo para alterar modo de operação do DAF	74
6.1	Sequência de pedido-resposta da API DAF encapsulada pelo PDAF-USB	86
6.2	Organização hierárquica da comunicação do PDAF-USB	87
6.3	Máquina de estados da Garantia de entrega	89
6.4	Máquina de estados da recepção do Enquadramento	90
7.1	Diagrama de caso de uso da SEF	92
7.2	Diagrama de sequência do processo de autorização de um DF-e	99
7.3	Diagrama de sequência do processo de validação de autorização gerada pelo DAF	100

Lista de Tabelas

2.1	Condições de guarda	27
2.2	Processos operacionais associados às transições de estado do DAF	27
2.3	Valores armazenados na região protegida	28
3.1	Sinalização visual referente aos estados do DAF	38
4.1	Casos de uso disponíveis em cada subestado do estado OPERAÇÃO	51
5.1	Conjunto de informações essenciais de uma NFC-e	58
5.2	Conjunto de informações essenciais de um BP-e	58
6.1	Pedidos da API DAF	77
6.2	Códigos das respostas geradas pelo DAF	78
6.3	Informações encaminhadas no pedido registrar	78
6.4	Informações encaminhadas na resposta do pedido registrar	79
6.5	Informações encaminhadas no pedido confirmarRegistro	80
6.6	Informações encaminhadas na resposta do pedido solicitarAutenticacao	80
6.7	Informações encaminhadas no pedido autorizarDFE	80
6.8	Informações encaminhadas na resposta do pedido autorizarDFE	81
6.9	Informações encaminhadas no pedido apagarAutorizacaoRetida	81
6.10	Informações encaminhadas no pedido removerRegistro	82
6.11	Informações encaminhadas na resposta do pedido removerRegistro	82
6.12	Informações encaminhadas no pedido confirmarRemocaoRegistro	82
6.13	Informações encaminhadas na resposta do pedido consultarInformacoes	83
6.14	Informações encaminhadas no pedido atualizarCertificado	84
6.15	Informações encaminhadas no pedido descarregarRetido	84
6.16	Informações encaminhadas na resposta do pedido descarregarRetido	84
6.17	Informações encaminhadas no pedido alterarModoOperacao	85
6.18	Informações encaminhadas na resposta do pedido alterarModoOperacao	85
6.19	Informações encaminhadas no pedido confirmarAlterarModoOperacao	86
6.20	Comandos de transporte do PDAF-USB	87
6.21	Formato do quadro PDAF-USB	87
6.22	Códigos de controle da subcamada Garantia de entrega do PDAF-USB	88
6.23	Quadro do comando enviarMensagem	90
6.24	Quadro do comando enviarBinario	90
6.25	Quadro da confirmação dos comandos enviarMensagem e enviarBinario	91

7.1	Descrição dos campos do CSR para registro de modelo de DAF	93
8.1	Relação dos Serviços <i>Web</i> providos pela SEF para o PAF do contribuinte	101
8.2	Cabeçalho das tabelas com definições de leiaute XML	104
8.3	Regras gerais de validação	105
8.4	Tabela de códigos de resultado de processamento	105
8.5	Tabela de códigos de rejeição de caso de uso	106
8.6	Leiaute da mensagem de entrada do método <code>iniciarRegistro</code>	107
8.7	Leiaute da mensagem de retorno do método <code>iniciarRegistro</code>	108
8.8	Conteúdo do <code>tkDesafio</code> da mensagem de retorno do <code>iniciarRegistro</code>	108
8.9	Códigos de rejeição da mensagem de entrada do método <code>iniciarRegistro</code>	108
8.10	Leiaute da mensagem de entrada do método <code>confirmarRegistro</code>	109
8.11	Conteúdo do <code>tkAut</code> da mensagem de entrada do método <code>confirmarRegistro</code>	109
8.12	Leiaute da mensagem de retorno do método <code>confirmarRegistro</code>	109
8.13	Conteúdo do <code>tkChaves</code> da mensagem de retorno do <code>confirmarRegistro</code>	110
8.14	Códigos de rejeição da mensagem de entrada do método <code>confirmarRegistro</code>	110
8.15	Leiaute da mensagem de entrada do método <code>removerRegistro</code>	111
8.16	Leiaute da mensagem de retorno do método <code>removerRegistro</code>	111
8.17	Conteúdo do <code>tkDesafio</code> da mensagem de retorno do <code>removerRegistro</code>	112
8.18	Códigos de rejeição da mensagem de entrada do método <code>removerRegistro</code>	112
8.19	Leiaute da mensagem de entrada do método <code>confirmarRemoverRegistro</code>	112
8.20	Conteúdo do <code>tkAut</code> da mensagem de entrada do <code>confirmarRemoverRegistro</code>	113
8.21	Leiaute da mensagem de retorno do método <code>confirmarRemoverRegistro</code>	113
8.22	Conteúdo do <code>tkEvento</code> da mensagem de retorno do <code>confirmarRemoverRegistro</code>	113
8.23	Códigos de rejeição da mensagem de entrada do método <code>confirmarRemoverRegistro</code>	114
8.24	Leiaute da mensagem de entrada do método <code>obterResultadoAutorizacao</code>	114
8.25	Leiaute da mensagem de retorno do método <code>obterResultadoAutorizacao</code>	115
8.26	Códigos de rejeição sobre a validação do processamento do fragmento DAF	115
8.27	Códigos de rejeição da mensagem de entrada do método <code>obterResultadoAutorizacao</code>	116
8.28	Leiaute da mensagem de entrada do método <code>encaminharDFeRejeitado</code>	117
8.29	Leiaute da mensagem de retorno do método <code>encaminharDFeRejeitado</code>	117
8.30	Códigos de rejeição da mensagem de entrada do método <code>encaminharDFeRejeitado</code>	118
8.31	Leiaute da mensagem de entrada do método <code>encaminharAutorizacoesRetidas</code>	118
8.32	Leiaute da mensagem de retorno do método <code>encaminharAutorizacoesRetidas</code>	119
8.33	Códigos de rejeição do método <code>encaminharAutorizacoesRetidas</code>	119
8.34	Leiaute da mensagem de entrada do método <code>consultarAutorizacaoApagar</code>	120
8.35	Leiaute da mensagem de retorno do método <code>consultarAutorizacaoApagar</code>	121
8.36	Códigos de rejeição sobre a validação do processamento do fragmento DAF	121
8.37	Códigos de rejeição da mensagem de entrada do método <code>consultarAutorizacaoApagar</code>	122
8.38	Leiaute da mensagem de entrada do método <code>avisarExtravio</code>	122
8.39	Leiaute da mensagem de retorno do método <code>avisarExtravio</code>	123
8.40	Códigos de rejeição da mensagem de entrada do método <code>avisarExtravio</code>	123
8.41	Leiaute da mensagem de entrada do método <code>alterarModoOperacao</code>	124
8.42	Leiaute da mensagem de retorno do método <code>alterarModoOperacao</code>	124
8.43	Conteúdo do <code>tkDesafio</code> da mensagem de retorno do <code>alterarModoOperacao</code>	125

8.44	Códigos de rejeição da mensagem de entrada do método <code>alterarModoOperacao</code> . . .	125
8.45	Leiaute da mensagem de entrada do método <code>confirmarModoOperacao</code>	125
8.46	Conteúdo <code>tkAut</code> da mensagem de entrada do <code>confirmarModoOperacao</code>	126
8.47	Leiaute da mensagem de retorno do método <code>confirmarModoOperacao</code>	126
8.48	Conteúdo do <code>tkModoOperacao</code> da mensagem de retorno do <code>confirmarModoOperacao</code>	126
8.49	Códigos de rejeição da mensagem de entrada do método <code>confirmarModoOperacao</code> .	127
8.50	Leiaute da mensagem de entrada do método <code>consultarVersaoSB</code>	127
8.51	Leiaute da mensagem de retorno do método <code>consultarVersaoSB</code>	128
8.52	Códigos de rejeição da mensagem de entrada do método <code>consultarVersaoSB</code>	128
8.53	Leiaute da mensagem de entrada do método <code>solicitarCertificado</code>	129
8.54	Leiaute da mensagem de retorno do método <code>solicitarCertificado</code>	129
8.55	Códigos de rejeição da mensagem de entrada do método <code>solicitarCertificado</code> . .	130
8.56	Leiaute da mensagem de entrada do método <code>consultarDispositivo</code>	130
8.57	Leiaute da mensagem de retorno do método <code>consultarDispositivo</code>	131
8.58	Códigos de rejeição da mensagem de entrada do método <code>consultarDispositivo</code> . .	131
8.59	Leiaute da mensagem de entrada do método <code>solicitarChavePAF</code>	132
8.60	Leiaute da mensagem de retorno do método <code>solicitarChavePAF</code>	132
8.61	Códigos de rejeição da mensagem de entrada do método <code>solicitarChavePAF</code>	133

Lista de Códigos

2.1	Exemplo de como gerar UUID versão 5 em Python 3.7	31
5.1	Exemplo de NFC-e que contém a autorização gerada DAF	59
6.1	Documento JSON para resposta do tipo simples	77
8.1	Exemplo de mensagem de requisição SOAP	102
8.2	Exemplo de mensagem de retorno SOAP	103
8.3	Exemplo de assinatura da mensagem de entrada	103
A.1	Documento JSON para pedidos sem assinatura digital e sem parâmetros adicionais .	137
A.2	Documento JSON para pedidos sem assinatura digital e com parâmetros adicionais .	137
A.3	Documento JSON para respostas sem assinatura digital e sem parâmetros	138
A.4	Documento JSON para respostas sem assinatura digital e com parâmetros adicionais	138
A.5	Documento JSON para pedidos com assinatura digital	139
A.6	Documento JSON para respostas com assinatura digital	139
A.7	Documento JSON com o <i>header</i> do <i>token</i> JWT utilizando chave RSA	140
A.8	Documento JSON com o <i>header</i> do <i>token</i> JWT utilizando chave EC	140
A.9	Documento JSON com o <i>header</i> do <i>token</i> JWE	141
B.1	Documento JSON para o pedido da mensagem consultarInformacoes	142
B.2	Documento JSON para a resposta da mensagem consultarInformacoes	142
B.3	Documento XML de entrada do método iniciarRegistro	143
B.4	Cabeçalho e conteúdo do <i>token</i> JWT que será incorporado no retorno do método iniciarRegistro	144
B.5	Documento XML de retorno do método iniciarRegistro	144
B.6	Documento JSON para o pedido da mensagem registrar	144
B.7	Cabeçalho e conteúdo do <i>token</i> JWT a ser assinado com a chave privada do DAF . .	145
B.8	Cabeçalho e conteúdo do <i>token</i> JWT a ser assinado com a chave de ateste	146
B.9	Documento JSON para a resposta da mensagem registrar	146
B.10	Documento XML de entrada do método confirmarRegistro	147
B.11	Cabeçalho e conteúdo do <i>token</i> JWT que será incorporado no retorno do método confirmarRegistro	148
B.12	Documento XML de retorno do método confirmarRegistro	148
B.13	Documento JSON para o pedido da mensagem confirmarRegistro	149
B.14	Documento JSON para a resposta da mensagem confirmarRegistro	149
B.15	Documento XML de entrada do método removerRegistro	150
B.16	Cabeçalho e conteúdo do <i>token</i> JWT que será incorporado no retorno do método removerRegistro	150
B.17	Documento XML de retorno do método removerRegistro	150

B.18 Documento JSON para o pedido da mensagem <code>removerRegistro</code>	151
B.19 Cabeçalho e conteúdo do <i>token</i> JWT que será incorporado na resposta da mensagem <code>removerRegistro</code>	151
B.20 Documento JSON para a resposta da mensagem <code>removerRegistro</code>	151
B.21 Documento XML de entrada do método <code>confirmarRemoverRegistro</code>	152
B.22 Cabeçalho e conteúdo do <i>token</i> JWT que será incorporado no retorno do método <code>confirmarRemoverRegistro</code>	152
B.23 Documento XML de retorno do método <code>confirmarRemoverRegistro</code>	152
B.24 Documento JSON para o pedido da mensagem <code>confirmarRemocaoRegistro</code>	153
B.25 Documento JSON para a resposta da mensagem <code>confirmarRemocaoRegistro</code>	153
B.26 Documento JSON para o pedido da mensagem <code>solicitarAutenticacao</code>	154
B.27 Documento JSON para a resposta da mensagem <code>solicitarAutenticacao</code>	154
B.28 Documento XML de uma NFC-e para o pedido da mensagem <code>autorizarDFE</code>	154
B.29 Fragmento XML com conjunto de informações essenciais de uma NFC-e para o pedido da mensagem <code>autorizarDFE</code>	154
B.30 Documento JSON para o pedido da mensagem <code>autorizarDFE</code>	155
B.31 Cabeçalho e conteúdo do <i>token</i> JWT que será incorporado na resposta da mensagem <code>autorizarDFE</code>	155
B.32 Documento JSON para a resposta da mensagem <code>autorizarDFE</code>	156
B.33 Documento XML de entrada do método <code>obterResultadoAutorizacao</code>	156
B.34 Documento XML de retorno do método <code>obterResultadoAutorizacao</code>	156
B.35 Documento JSON para o pedido da mensagem <code>apagarAutorizacaoRetida</code>	157
B.36 Documento JSON para a resposta da mensagem <code>apagarAutorizacaoRetida</code>	157
B.37 Documento JSON para o pedido da mensagem <code>consultarInformacoes</code>	157
B.38 Documento JSON para a resposta da mensagem <code>consultarInformacoes</code>	158
B.39 Documento JSON para o pedido da mensagem <code>descarregarRetido</code>	158
B.40 Documento JSON para a resposta da mensagem <code>descarregarRetido</code>	159
B.41 Documento XML de entrada do método <code>encaminharAutorizacoesRetidas</code>	159
B.42 Documento XML de retorno do método <code>encaminharAutorizacoesRetidas</code>	160
B.43 Documento XML de entrada do método <code>consultarApagar</code>	160
B.44 Documento XML de retorno do método <code>consultarApagar</code>	160
B.45 Documento JSON para o pedido da mensagem <code>apagarAutorizacaoRetida</code>	161
B.46 Documento JSON para a resposta da mensagem <code>apagarAutorizacaoRetida</code>	161

Lista de Algoritmos

1	Estado Ocioso da máquina de estados finitos da Garantia de entrega	163
2	Estado Espera da máquina de estados finitos da Garantia de entrega	164
3	Estado Ocioso da máquina de estados finitos da camada de Enquadramento	165
4	Estado Tamanho da máquina de estados finitos da camada de Enquadramento	165
5	Estado RX da máquina de estados finitos da camada de Enquadramento	166

1 Introdução

O projeto **Dispositivo Autorizador Fiscal (DAF)** surgiu de uma necessidade da **SEF** para adoção da **Nota Fiscal de Consumidor Eletrônica (NFC-e)** no estado de Santa Catarina. A concepção desse projeto foi guiada pelo §7º do ajuste **SINIEF 15/2018 (CONFAZ, 2018)** o qual indica que a emissão e autorização da **Nota Fiscal de Consumidor Eletrônica (NFC-e)** em Santa Catarina será realizada por meio de equipamento desenvolvido e autorizado para uso fiscal, comandado por meio de programa aplicativo desenvolvido por empresa credenciada pela respectiva administração tributária.

O **Dispositivo Autorizador Fiscal (DAF)** tem por objetivo ser um equipamento de baixo custo, com premissas robustas de segurança e operado por meio do **Programa Aplicativo Fiscal (PAF)** para obter autorização, junto à **Secretaria de Estado da Fazenda de Santa Catarina (SEF)**, de **Documentos Fiscais Eletrônicos (DF-e)** que possam ser emitidos em modo de contingência *offline*. Dessa forma, comparando com os atuais dispositivos fiscais usados no Brasil, o projeto **DAF** pretende simplificar o equipamento, procedimentos e ainda assim garantir as prerrogativas de fiscalização e controle. Essa solução trará os seguintes benefícios aos atores envolvidos:

- **Contribuinte:** Custo total de propriedade reduzido, considerando todos os custos envolvidos durante o ciclo de vida do DAF (aquisição, manutenção e credenciamento);
- **Software House:** Simplicidade na criação ou integração do **PAF**;
- **Fabricante de DAF:** Margem para agregar funcionalidades e gerar diferentes modelos de negócio.

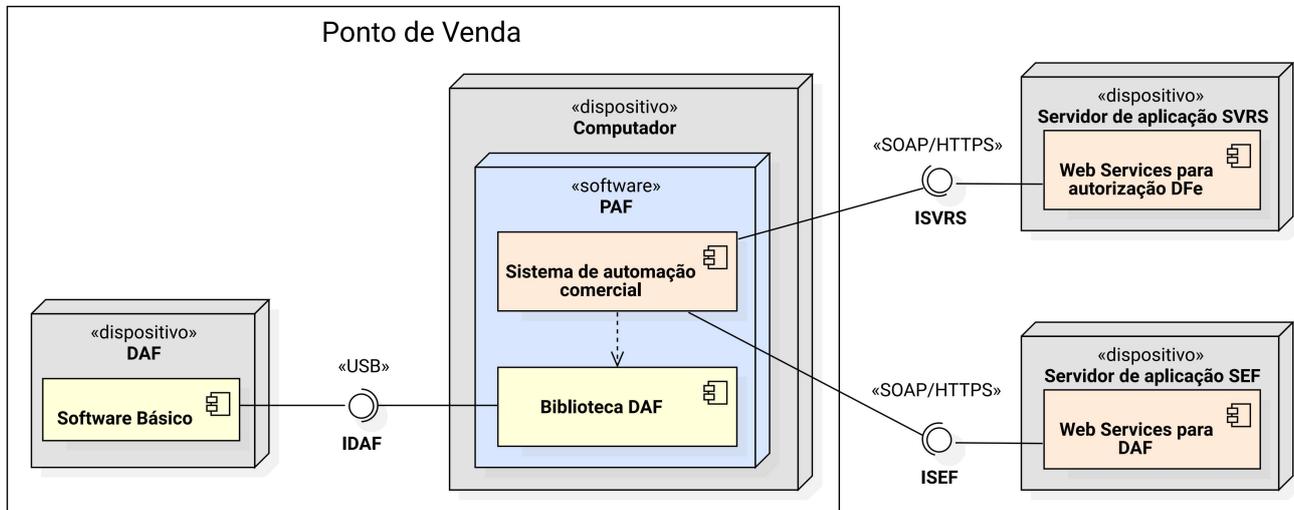
A modalidade de contingência *offline* pode ser usada quando o **contribuinte** não tem conexão com a **Secretaria de Estado da Fazenda (SEFAZ)** de origem ou a comunicação apresenta grande lentidão, seja por problemas técnicos na **SEFAZ** ou por problema de conexão à Internet no lado do contribuinte. De acordo com **ENCAT (2016)**, é de exclusiva escolha do contribuinte a opção por esta modalidade de contingência, não sendo necessária autorização prévia do Fisco, porém este pode solicitar esclarecimento e até proibir esse tipo de emissão em caso de uso em demasia e sem justificativa aceitável.

De acordo com a decisão do **Grupo Especialista Setorial em Automação Comercial da SEF (GESAC)**, o DAF deverá ser capaz de autorizar os seguintes documentos **Bilhete de Passagem Eletrônico (BP-e)** (**ENCAT, 2019b**) e **Nota Fiscal de Consumidor Eletrônica (NFC-e)** (**ENCAT, 2019a**), uma vez que a emissão desses pode ser feita de modo *offline* com posterior envio para **SEFAZ**.

Na **Figura 1.1** é apresentado um diagrama de implantação **UML** (**COOK et al., 2017**) com as principais entidades do projeto DAF e como essas se relacionam. O DAF deverá estar conectado na porta **USB** do computador onde o **PAF** será executado. A autorização de **DF-e** deverá ser feita junto à **SEFAZ**

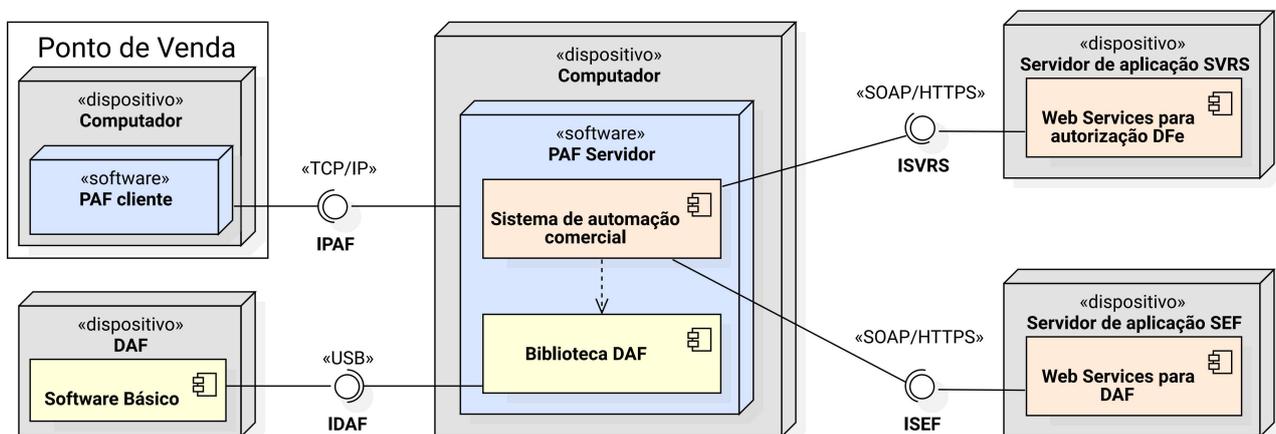
autorizadora, no caso a **SEFAZ Virtual do Rio Grande do Sul (SVRS)** ou a própria **SEF**, quando essa vier a ser uma autorizadora. A **SEF** proverá um conjunto de **Serviços Web (Web Services)** específicos para atuação com o **DAF**, o que inclui, a validação de autorizações emitidas por esse.

Figura 1.1: Entidades do projeto DAF



O **Programa Aplicativo Fiscal** consiste no *software* capaz de comandar o **DAF** para emissão e autorização de **DF-e** junto à **SEFAZ** e também de executar outras rotinas comuns dos **sistemas de automação comercial**. Caberá ao **contribuinte** escolher se deseja ter um **DAF** fisicamente conectado em cada **PDV** ou compartilhar um mesmo **DAF** por vários **PDVs** (veja **Seção 5.8**). Nesse último caso, o **PAF** obrigatoriamente deverá seguir o modelo cliente e servidor (veja **Figura 1.2**).

Figura 1.2: Diagrama de implantação com o PAF no modelo cliente e servidor



Esse documento tem como audiência os fabricantes de **DAF** e os desenvolvedores de **PAF**. Esse documento tem como escopo a especificação técnica de requisitos para o **DAF**, o que inclui:

- Processos operacionais que o **DAF** está apto a realizar;
- Especificação do *hardware* e *software* do **DAF**;
- Protocolo de comunicação entre **DAF** e **PAF**;
- Serviços providos pela **SEF** para interação com o **DAF**;
- Protocolo de comunicação entre **PAF** e os **Serviços Web** da **SEF**.

Não faz parte do escopo desse documento apresentar a especificação de requisitos técnicos para o desenvolvimento do PAF. Também não faz do escopo desse documento indicar como a SEF deverá implementar os Serviços *Web* ou mesmo os sistemas de apoio para fabricantes de DAF, desenvolvedores de PAF ou entidades certificadoras de DAF.

1.1 Terminologia para indicar os níveis de exigência

Nesse documento é feito uso das palavras DEVE, NÃO DEVE, PODERIA, NÃO PODERIA, PODE e suas formas no plural para indicar o nível de exigência daquilo que está sendo especificado. Essas palavras são traduções literais das palavras *MUST*, *MUST NOT*, *SHOULD*, *SHOULD NOT* e *MAY* apresentadas na RFC 2119 (BRADNER, 1997) e devem ser interpretadas como descritas naquele documento.

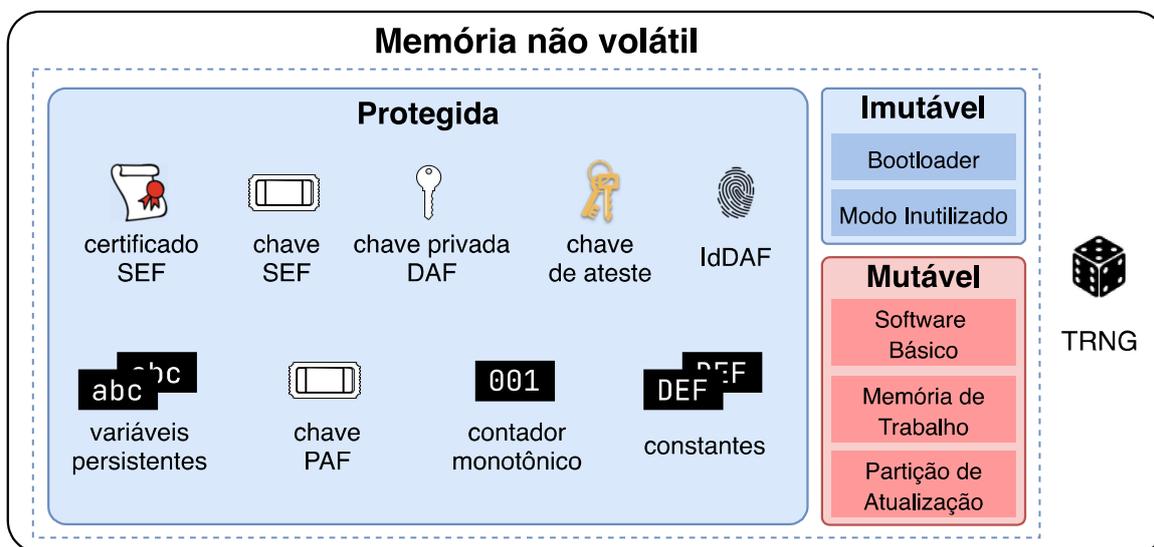
2 Visão geral do DAF

O Dispositivo Autorizador Fiscal (DAF) tem por objetivo ser um equipamento de baixo custo, com premissas robustas de segurança e operado por meio do PAF para obter autorização, junto à Secretaria de Estado da Fazenda (SEFAZ), de Documentos Fiscais Eletrônicos (DF-e). O DAF consiste de um dispositivo passivo que só reage mediante a um estímulo do PAF. Ou seja, o DAF só enviará uma mensagem se antes receber um pedido do PAF.

Neste capítulo é apresentada uma visão de alto nível do DAF. De uma forma geral, são descritos os principais componentes, os artefatos criptográficos (Seção 2.1), os mecanismos de segurança (Seção 2.1), os estados de operação (Seção 2.2) e a arquitetura da memória não volátil (Seção 2.3). Para mais detalhes sobre a implementação do *hardware* e do *Software Básico* (SB), consultar o Capítulo 3 e o Capítulo 4, respectivamente.

Na Figura 2.1 é apresentada uma visão geral da arquitetura do DAF com os principais componentes e artefatos.

Figura 2.1: Visão geral da arquitetura do DAF.



Abaixo são descritos os principais componentes do DAF:

- **Bootloader** - O *bootloader* do DAF, denominado apenas de *bootloader* ao longo deste documento, reúne o sistema básico executado após o processo de inicialização do microcontrolador. O *bootloader* do DAF pode coexistir com um *bootloader* embutido de fábrica da ROM. Neste caso, o *bootloader* do DAF assume a execução do processador imediatamente após a execução do *bootloader* da ROM;

- **Modo inutilizado** - conjunto de rotinas que implementam as funcionalidades do estado INUTILIZADO;
- **Software Básico (SB)** - conjunto de rotinas, residentes no DAF que implementa as funções de controle fiscal;
- **Memória de Trabalho (MT)** - conjunto de recursos em *hardware* destinado à gravação de dados para apoio do funcionamento do *Software Básico (SB)*;
- **Partição de atualização** - região de memória reservada para armazenar o *Software Básico Candidato (SBC)* durante o processo de atualização segura;
- **True Random Number Generator (TRNG)** - componente físico que gera uma sequência de símbolos aleatórios que não pode ser prevista.

2.1 Artefatos

Abaixo são descritos os artefatos do DAF de acordo com o momento em que serão inseridos na memória do DAF.

- **Artefatos armazenados durante a manufatura:**
 - **Chave de ateste** - chave privada incluída na memória segura do dispositivo em tempo de manufatura. Essa chave é usada durante o processo de registro do DAF junto à SEF. A chave de ateste deverá ser única para cada modelo de DAF;
 - **Certificado digital da SEF** - certificado digital da Secretaria de Estado da Fazenda de Santa Catarina (SEF) incluído na memória segura do dispositivo em tempo de manufatura. Deverá ser usado pelo *bootloader* e pelas rotinas internas do *Software Básico (SB)*;
 - **Identificador único do DAF (IdDAF)** - número único por dispositivo incluído na memória segura do dispositivo em tempo de manufatura. Esse identificador deve ser um *Universally Unique Identifier (UUID)*;
 - **Contador monotônico** - contador que incrementa de forma monotônica a cada operação de autorização sobre DF-e realizada pelo DAF.
- **Artefatos gerados e armazenados durante o funcionamento:**
 - **Chave privada do DAF** - chave privada gerada pela rotina de registro do DAF junto à SEF;
 - **Chave SEF** - número arbitrário gerado pela SEF e único para cada DAF, após processo de registro do DAF;
 - **Chave PAF** - número arbitrário gerado pela SEF e único para cada PAF, após processo de registro do DAF;
 - **Modo de operação do DAF** - indica se o DAF é operado por apenas um PDV ou compartilhado por mais de um PDV.

A **chave de ateste** é usada obrigatoriamente pelo processo de registro do DAF junto à SEFAZ (veja [Seção 5.1](#)) para que essa última tenha certeza que está interagindo com um **DAF** genuíno e certificado.

O [certificado digital da SEF](#) será usado pelo [DAF](#) para garantir a autenticidade das mensagens geradas pela SEF em alguns casos de uso e durante a atualização segura para verificar se o [SB](#) está íntegro e é autêntico (veja [Seção 5.6](#)). Além disso, também será utilizado no processo de atualização do próprio certificado (veja [Seção 5.7](#)).

A [chave privada do DAF](#) é gerada dentro do ambiente de execução seguro após o processo de registro do DAF junto à SEF (veja [Seção 5.1](#)). Assinaturas emitidas com a [chave privada do DAF](#) permitirão à SEF ter certeza que está interagindo com o dispositivo registrado por um determinado [contribuinte](#). Essa chave será usada em alguns casos de uso, como para troca segura da [chave SEF](#) entre a SEF e o DAF.

O [contador monotônico](#) armazena o total de operações de autorização realizadas pelo DAF. Além de ser parte da entrada das [rotinas criptográficas](#), o [contador monotônico](#) deve ser encaminhado à SEFAZ junto com cada mensagem referente às operações fiscais (veja [Seção 5.2](#)).

A [chave SEF](#) e [chave PAF](#) serão geradas após o DAF ter passado pelo processo de registro (veja [Seção 5.1](#)). A [chave SEF](#) será mantida somente no DAF e na SEF. A [chave PAF](#) será mantida no DAF, no PAF e na SEF. Caso o PAF venha a perdê-la, o contribuinte poderá recorrer à rotina específica da SEF para recuperar a cópia da mesma (veja [Subseção 7.6.5](#) e [Subseção 8.14.1](#)).

O [modo de operação do DAF](#) indica se o DAF é operado por um único [PDV](#) ou se é compartilhado por mais de um [PDV](#). A alteração do modo de operação do DAF fica a critério do contribuinte e esse poderá fazê-la sempre que desejado, durante ou após o registro do DAF e de acordo com a legislação vigente.

2.2 Estados de operação

O DAF pode assumir os estados BOOTLOADER, INUTILIZADO e os subestados INATIVO, PRONTO e BLOQUEADO, também chamados de estados por questões de simplificação da nomenclatura. Abaixo a descrição sucinta de cada um desses estados.

- **BOOTLOADER:** Esse é o estado de inicialização do [DAF](#) após energizado ou reiniciado. Nesse estado, acontecem as verificações iniciais do sistema e o processo final da atualização quando há um [Software Básico Candidato \(SBC\)](#) na [partição de atualização](#) (veja [Subseção 2.4.6](#));
- **INUTILIZADO:** A transição para esse estado deve ocorrer a partir de qualquer estado ou subestado assim que for detectada alguma tentativa de violação. Esse estado deve ser irreversível, ou seja, é persistido em memória não volátil o indicador VIOLADO o qual é utilizado como condição de guarda e deve levar ao estado INUTILIZADO imediatamente depois do estado BOOTLOADER. As operações executadas nesse estado são bastante limitadas (veja [Subseção 2.4.7](#));
- **INATIVO:** Esse é o estado do padrão de fábrica e é considerado como não associado a nenhum [contribuinte](#). O DAF só deve sair desse estado após um registro bem sucedido junto à SEF (veja [Seção 5.1](#)) e só retornará após o processo de remoção do registro (veja [Seção 5.5](#)), o qual pode ocorrer somente se não houver nenhuma autorização fiscal pendente na [Memória de Trabalho](#);
- **PRONTO:** Nesse estado é possível executar todos os casos de uso relacionados com as autorizações fiscais. A transição para o estado BLOQUEADO deve ocorrer caso o limite de

autorizações retidas seja atingido, ou seja, $\text{numDFe} \geq \text{Max}$ (veja Seção 5.2 e Caso de Uso UC-4.3);

- BLOQUEADO: O DAF não poderá emitir nenhuma autorização fiscal nesse estado. Este estado pode ser alcançado por meio de um auto-bloqueio. Dessa forma, para sair desse estado, é necessário apagar pelo menos uma autorização retida (veja Caso de Uso UC-4.2).

A Figura 2.2 ilustra a máquina de estados comportamental do DAF no padrão UML. Além dos estados, é possível visualizar os casos de uso que são gatilhos (*triggers*) e efeitos (*behavior expression*) das transições entre os estados. Também é possível visualizar, entre colchetes, as condições de guarda (*guards*) significativas às transições entre os estados. Essas condições de guarda são detalhadas na Tabela 2.1, e não tem a intenção de cobrir todos os detalhes dos processos operacionais do DAF, que devem ser consultados no Capítulo 5.

Figura 2.2: Máquina de estados do Dispositivo Autorizador Fiscal

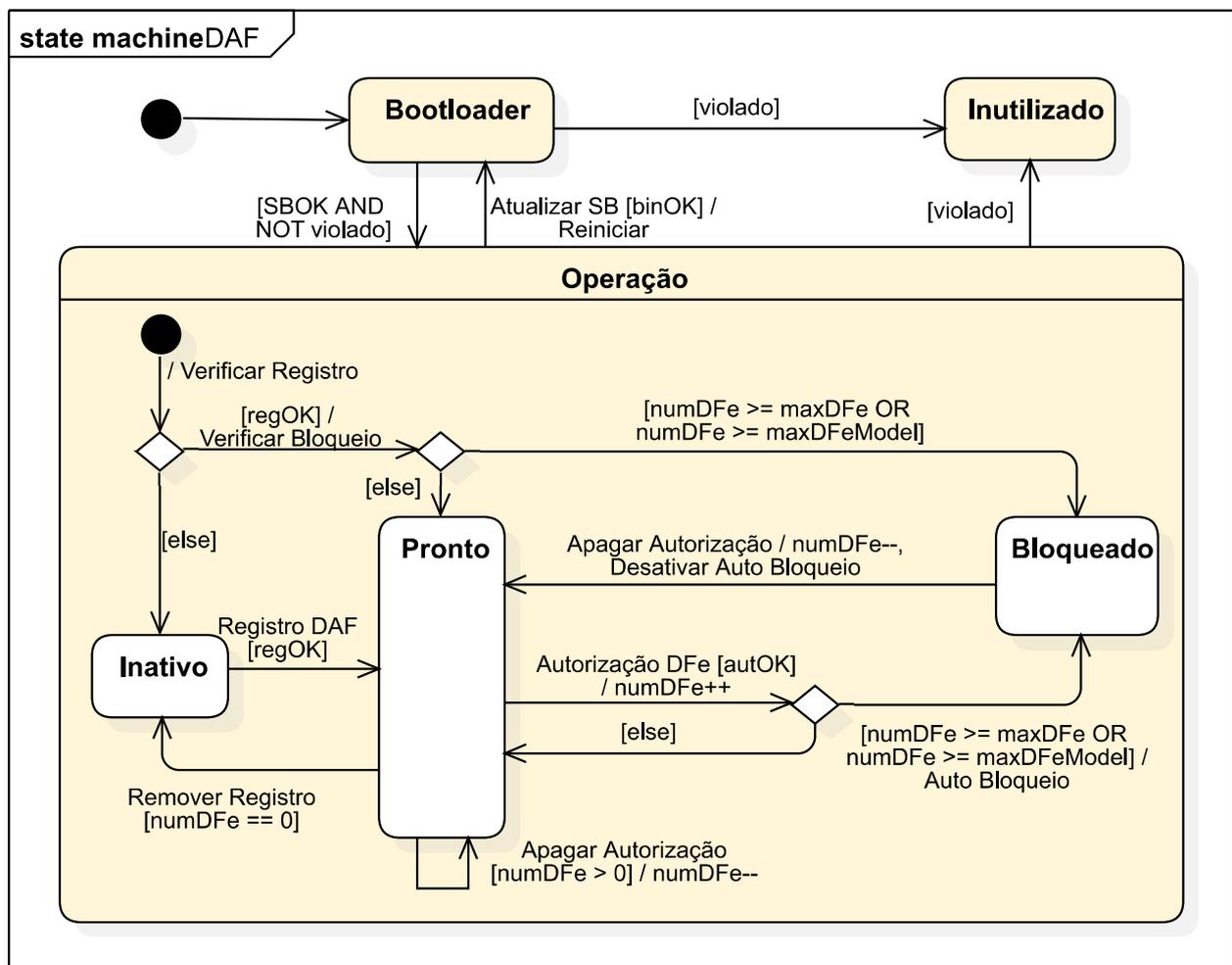


Tabela 2.1: Condições de guarda

Nome	Valor inicial	Descrição
SBOK	N.A. ¹	Resultado do processo de validação do SB na inicialização do sistema.
binOK	N.A.	Resultado do processo de verificação da integridade e da autenticidade do SBC.
autOK	N.A.	Resultado da autenticação do PAF.
numDFe	0	Quantidade de autorizações retidas no DAF.
maxDFeModel	A definir	Limite máximo de autorizações que o modelo de DAF é capaz de reter em memória. Definido pelo fabricante e relacionado com o tamanho da memória do dispositivo.
maxDFeSef	∞	Previsão de um limite máximo de autorizações retidas que pode ser definido pela SEF e incluída em uma futura atualização do SB.
regOK	Falso	Indicador do registro do DAF junto à SEF.
violado	Falso	Indicador que foi detectada uma tentativa de violação no DAF. A alteração do valor para verdadeiro é irreversível.

A Tabela 2.2 reúne todas as transições entre os estados que estão associadas aos processos operacionais do DAF (veja Capítulo 5).

Tabela 2.2: Processos operacionais associados às transições de estado do DAF

Gatilho	Transição	Descrição
Registro do DAF	INATIVO → PRONTO	Sucesso no processo de registro do DAF junto à SEF (veja Seção 5.1).
Remover Registro	PRONTO → INATIVO	Processo de remoção do registro junto à SEF (veja Seção 5.5), no qual não pode haver autorizações retidas na memória do DAF (<code>numDFe == 0</code>).
Autorização DFe	PRONTO → BLOQUEADO	Processo de autorização de um DF-e (veja Seção 5.2) quando pelo menos um dos limites máximos (<code>maxDFe</code> ou <code>maxDFeModel</code>) é alcançado e o auto-bloqueio é ativado (veja Caso de Uso UC-4.3).
Apagar Autorização	BLOQUEADO → PRONTO	Processo de remoção de um DF-e (veja Seção 5.3) estando no estado BLOQUEADO devido ao auto-bloqueio, o qual é desativado (veja UC-4.8).
Atualizar SB	OPERAÇÃO → BOOTLOADER	Processo de atualização do SB (veja Seção 5.6), quando o <i>Software Básico Candidato</i> é válido para atualização.

O funcionamento completo do DAF no estado OPERAÇÃO é especificado no Capítulo 4, Capítulo 5 e Capítulo 6. A relação dos casos de uso disponíveis nos subestados PRONTO, INATIVO e BLOQUEADO pode ser encontrada na Seção 4.3.

¹Não se aplica (N.A.). O valor é o resultado de uma função e não persiste.

2.3 Arquitetura de memória

Os componentes de *software*, artefatos, variáveis persistentes e constantes armazenadas na memória não volátil do DAF possuem diferentes exigências em relação ao momento que são escritas na memória, a mutabilidade, ao nível de sigilo e a segurança. Nesse sentido, dividiu-se a memória não volátil em três regiões de armazenamento: imutável, mutável e protegida.

Os requisitos da região imutável são especificados em detalhes na [Subseção 2.4.3](#). De forma geral, essa região armazena o código do *bootloader*, que é responsável pelo estado inicial homônimo do DAF, e o código que implementa as funcionalidades esperadas para o estado INUTILIZADO.

Os requisitos da região mutável são especificados em detalhes na [Subseção 2.4.4](#). Essa região é composta por três partições cujos conteúdos são modificáveis durante a operação, ou seja, após manufatura do DAF. A **Memória de Trabalho (MT)** é usada para armazenar as informações recebidas do PAF durante as autorizações de DF-e (veja [Caso de Uso UC-4.6](#)). Enquanto as outras duas partições armazenam o SB e, quando for o caso, a imagem de atualização, ou seja, o *Software Básico Candidato*.

A região protegida se diferencia das outras regiões especificadas por exigir o emprego de um dispositivo que tenha proteção física à violações, sensores antiviolação e capacidade de resposta no caso de uma violação ser detectada. Para essa região, os mecanismos de proteção devem ser intra-chip e incluem sensores ambientais e proteção contra ataques internos e externos. No caso da detecção de tentativa de violação, o material criptográfico sensível deve ser apagado. Os requisitos para essa região são especificados na [Subseção 2.4.5](#).

A região protegida deverá armazenar as constantes, que são valores armazenados em tempo de manufatura e não podem ser alterados durante toda a vida útil do DAF, e as variáveis persistentes, que são valores armazenados durante o funcionamento e devem persistir independente da interrupção de energia. Esses valores são consultados pelo SB e pelo *bootloader* para definir o comportamento do DAF. A [Tabela 2.3](#) lista os valores armazenados na região protegida.

Tabela 2.3: Valores armazenados na região protegida

Tipo	Nome	Constante	Variável Persistente
Condições de guarda (veja Tabela 2.1)	maxDFeModel	☑	
	maxDFe		☑
	regOK		☑
	numDFe		☑
	violado		☑
Artefatos (veja Seção 2.1)	Certificado digital da SEF		☑
	Chave privada do DAF		☑
	Chave SEF		☑
	Chave PAF		☑
	Contador monotônico		☑
	Chave de ateste	☑	
	IdDAF	☑	

	Modo de operação do DAF	☑
Parâmetros de atualização (veja Seção 5.6)	Resumo criptográfico do SB	☑
	Versão do SB	☑
	Falhas de atualização	☑
	CNPJ do fabricante do DAF	☑
	Modelo DAF	☑

2.4 Requisitos da arquitetura do DAF

Os requisitos com relação ao *hardware* do DAF foram divididos em duas categorias: i) requisitos da arquitetura, que são apresentados na sequência e possuem um caráter mais abstrato e indiferente aos detalhes estruturais; ii) requisitos da organização, que são apresentados no [Capítulo 3](#) e trazem os detalhes estruturais para a implementação do hardware. A lista de requisitos tem a numeração contínua entre os dois capítulos para facilitar a referência da especificação, implementação e homologação do DAF.

2.4.1 Requisitos criptográficos

Nesta seção são apresentados os algoritmos que DEVEM ser usados por DAF, PAF e SEF, em atividades como cifrar, decifrar, assinar e gerar [resumos criptográficos](#).

1. Chave de ateste DEVE:

1.1. fazer uso do algoritmo [RSA](#) e ter o tamanho de 4.096 bits; ou

1.2. fazer uso do algoritmo [Elliptic Curve \(EC\)](#) e a curva deve ser a P-521 ou a P-384 ([NIST, 2013](#)):

2. Chave privada do DAF DEVE:

2.1. fazer uso do algoritmo [RSA](#) e ter o tamanho de 2.048 bits; ou

2.2. fazer uso do algoritmo [EC](#) e a curva deve ser a P-256 ([NIST, 2013](#)).

3. As assinaturas digitais, quando usada a chave de ateste, DEVEM ser geradas dentro do ambiente de execução do microcontrolador seguro.

3.1. A suíte de assinatura DEVE ser [sha512WithRSAEncryption](#) ([MORIARTY et al., 2016](#)), [sha512WithECDSA](#) ou [sha384WithECDSA](#) quando usar chaves RSA, chaves EC com as curvas P-521 ou P-384, respectivamente.

4. As assinaturas digitais, quando usada a chave privada do DAF, DEVEM ser geradas dentro do ambiente de execução do microcontrolador seguro.

4.1. A suíte de assinatura DEVE ser [sha256WithRSAEncryption](#) ([MORIARTY et al., 2016](#)) ou [sha256WithECDSA](#) quando usar chaves RSA ou chaves EC com a curva P-256, respectivamente.

5. Os resumos criptográficos DEVEM ser gerados com a função SHA-256 ([NIST, 2015](#)).

6. Chave SEF é um valor arbitrário de 512 bits e DEVE ser mantida somente no DAF e na SEF.

7. **Chave PAF** é um valor arbitrário de 512 bits e DEVE ser mantida no DAF, no PAF e na SEF.
8. A cifragem de dados, quando usadas chaves **RSA**, DEVE:
 - 8.1. Fazer uso do esquema de cifragem **RSAES-OAEP** (MORIARTY et al., 2016);
 - 8.2. Fazer uso do *Mask Generation Function 1* (MGF1) (MORIARTY et al., 2016) com a função *hash* criptográfica **SHA-256**.
9. A cifragem de dados, quando usadas chaves **EC**, DEVE:
 - 9.1. Fazer uso do esquema **ECIES** (ANSI, 2001);
 - 9.2. Fazer uso do *Elliptic-curve Diffie–Hellman* (ECDH) como protocolo de estabelecimento de chave;
 - 9.3. Fazer uso do **AES-128-CBC-HMAC-SHA-256** como algoritmo de cifragem.
10. O **certificado digital da SEF** seguirá as especificações da **ICP-Brasil** (ICP-BRASIL, 2019, 2020), porém PODE ser auto-assinado (quando incluído em tempo de manufatura do DAF) ou PODE ter sido emitido por uma **Autoridade Certificadora (AC)** mantida ou indicada pela SEF que PODE não fazer parte da **ICP-Brasil**.
 - 10.1. A **chave pública** contida no certificado poderá ser uma chave **RSA** 4.096 bits ou uma chave **EC** com a curva **P-521** ou a **P-384**.
11. Todo material criptográfico sensível, como a **chave privada do DAF**, **chave de ateste** e **chave SEF** NÃO DEVE ser exportado ou ficar visível fora do ambiente de execução do microcontrolador seguro.
12. O código de autenticação de mensagem com chave *Hash-based Message Authentication Code* (**HMAC**) (KRAWCZYK; BELLARE; CANETTI, 1997), combinado com a função **SHA-256** (NIST, 2015), será usado por alguns casos de uso do DAF.
 - 12.1. Na interação entre DAF e SEF, a **chave SEF** DEVE ser usada como a chave secreta do **HMAC**;
 - 12.2. Na interação entre PAF e DAF, a chave secreta do **HMAC** DEVE ser a **chave PAF**.
13. O **contador monotônico** DEVE ter no mínimo 16 bits e reiniciar a contagem após estourar a representação.

2.4.2 Requisitos do identificador único do DAF

O **Identificador único do DAF (IdDAF)** permitirá à SEF identificar de forma inequívoca um DAF.

14. O **IdDAF** DEVE ser um *Universally Unique Identifier* (**UUID**) (LEACH; MEALLING; SALZ, 2005) da versão 1, 4 ou 5.
 - 14.1. Se optar pela versão 5 do **UUID**, então o fabricante do DAF DEVE usar seu nome de domínio na Internet (ex: `fabricante.exemplo.com.br`) como o espaço de nomes (*namespace*). O fabricante PODE escolher os valores para os nomes para cada DAF (ex: `modeloA+1234`). Na **Listagem 2.1** é apresentado um exemplo na linguagem Python de como gerar um **UUID** versão 5 para um DAF.

Listagem 2.1: Exemplo de como gerar UUID versão 5 em Python 3.7

```
1 import uuid
2 # Criar o namespace da versão 5 com o nome de domínio do fabricante
3 dominio = uuid.uuid5(uuid.NAMESPACE_DNS, 'fabricante.exemplo.com.br')
4
5 # Criar uuid a partir do domínio e name. No caso, name é uma string única por DAF
6 daf_modeloa_serie_1234 = uuid.uuid5(dominio, 'modeloA+1234')
```

15. O **IdDAF** PODE ser provido pelo fabricante do *chip* desde que seja imutável ou DEVE ser inserido, em tempo de manufatura do DAF, na região protegida de memória como constante (veja Tabela 2.3).

2.4.3 Requisitos da memória imutável

16. A região de memória imutável DEVE ser não volátil.
17. DEVE ser escrita somente em tempo de manufatura.
18. DEVE ficar bloqueada para reescrita e para apagamento de maneira irreversível após a manufatura.
19. DEVE armazenar a imagem do *bootloader* (veja Subseção 2.4.6).
20. DEVE armazenar o modo inutilizado (veja Subseção 2.4.7).

2.4.4 Requisitos da memória mutável

21. A região de memória mutável DEVE prever as partições **MT**, de armazenamento do **SB** e a partição de atualização.
22. DEVE ser não volátil.
23. PODE ser implementada por um ou mais componentes físicos de memória.
24. A partição **MT**:
 - 24.1. DEVE ser utilizada para armazenar as informações fiscais referente ao caso de uso Autorizar DF-e (UC-4.6) até a sua devida remoção (veja UC-4.2);
 - 24.2. DEVE possuir capacidade mínima de armazenar \maxDFe autorizações (veja Tabela 2.1);
 - 24.3. DEVE possuir vida útil para armazenar no mínimo $10.000 \times \maxDFe$ de autorizações;
 - 24.4. PODE ser implementada por um *chip* externo ao microcontrolador.
25. A partição do *Software Básico*:
 - 25.1. DEVE permitir escrita somente pelo *bootloader*;
 - 25.2. DEVE conter exclusivamente as instruções do **SB**.
26. A partição de atualização PODE ser implementada por um *chip* externo ao microcontrolador.
27. A **MT** e a partição de atualização PODEM ser implementadas no mesmo *chip*.

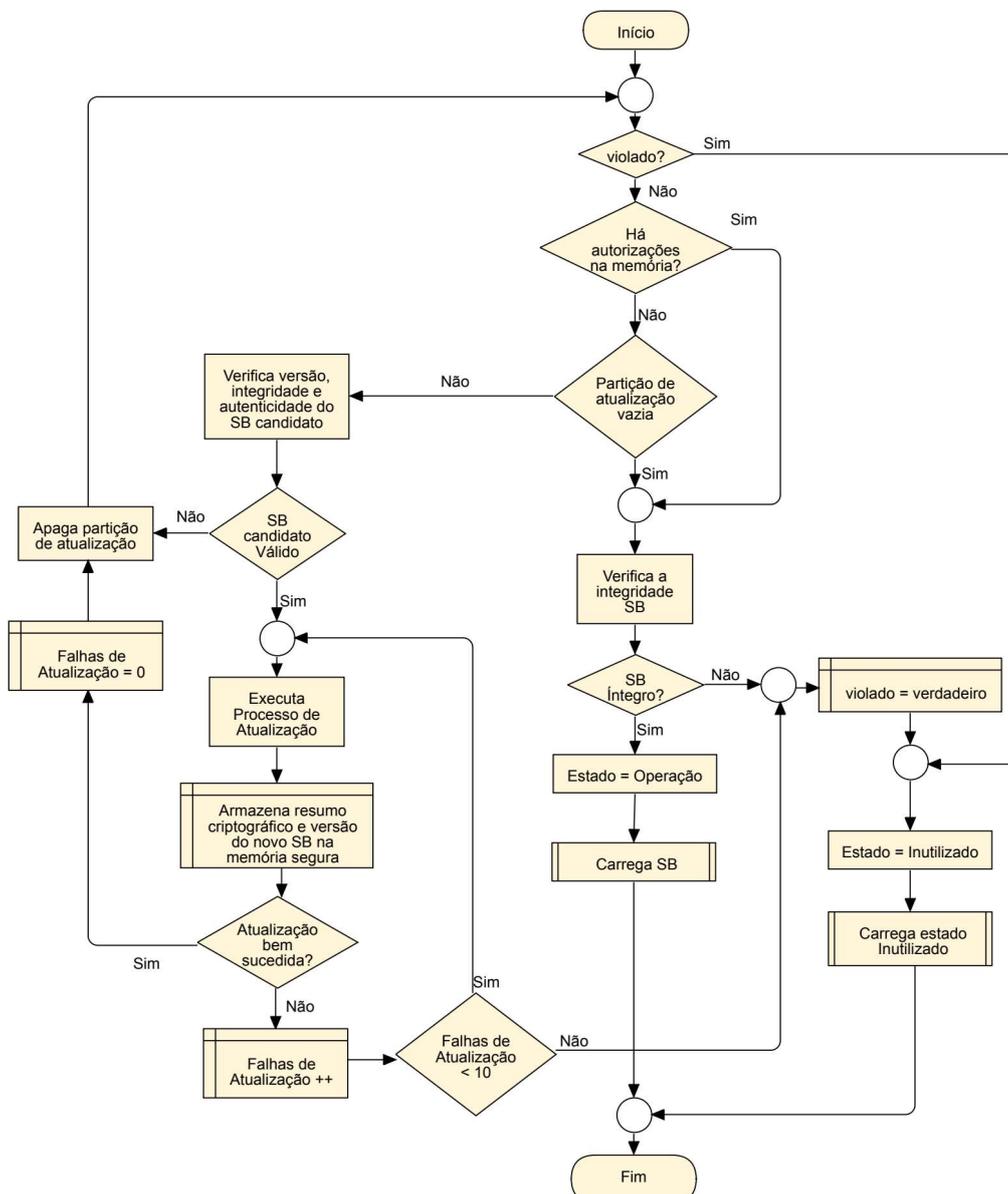
2.4.5 Requisitos da memória protegida

28. A região de memória protegida DEVE ser não volátil.
29. DEVE possuir mecanismos para atender os requisitos de armazenamento apresentados na Tabela 2.3.
30. DEVE possuir mecanismos anti violação para proteção, detecção e reação.
31. DEVE ter as *chave privada do DAF*, *chave de ateste* e *chave SEF* apagadas imediatamente em caso de violação.

2.4.6 Requisitos do *bootloader*

As operações executadas pelo *bootloader* são responsáveis pelo comportamento do estado homônimo. Sendo responsável pelas verificações iniciais do sistema e o processo final da atualização segura de uma nova versão do SB. O comportamento do *bootloader* é apresentado no fluxograma da Figura 2.3.

Figura 2.3: Fluxograma do comportamento do *bootloader*



Dessa forma, os requisitos do *bootloader* são os seguintes:

32. DEVE ser o único ponto de entrada após o reinício do DAF.
33. DEVE ser armazenado na região imutável (veja [Subseção 2.4.3](#)).
34. DEVE implementar o comportamento especificado na [Figura 2.3](#).
35. DEVE ter um contador de tentativas de atualização de SB.
 - 35.1. O contador de tentativas de atualização de SB DEVE ir para o valor 0 sempre que uma tentativa de atualização for bem-sucedida.
 - 35.2. Se o contador de tentativas de atualização de SB atingir o valor 10, o DAF DEVE ir para o estado INUTILIZADO.

2.4.7 Requisitos do modo inutilizado

36. O modo inutilizado DEVE ser armazenado na memória imutável (veja [Subseção 2.4.3](#)).
37. DEVE ser executado imediatamente após a detecção de uma violação.
38. DEVE ser irreversível e persistente.
39. DEVE implementar comunicação unidirecional do DAF para o *host*, pela interface de comunicação definida na [Seção 3.6](#).
40. NÃO DEVE implementar nenhum protocolo interativo, incluindo o protocolo descrito no [Capítulo 6](#).
41. DEVE enviar uma única vez, 30 segundos após entrar no estado INUTILIZADO, as informações abaixo na mesma ordem que aparecem e DEVEM ser representadas como uma cadeia de caracteres hexadecimais, separadas pelo caractere de barra vertical (*pipe*):
 - 41.1. Conteúdo da partição do SB;
 - 41.2. Conteúdo da MT;
 - 41.3. Os seguinte valores armazenados na memória protegida:
 - 41.3.1. `maxDFeModel`;
 - 41.3.2. `maxDFe`;
 - 41.3.3. `regOK`;
 - 41.3.4. `numDFe`;
 - 41.3.5. contador monotônico;
 - 41.3.6. `IdDAF`;
 - 41.3.7. modo de operação do DAF;
 - 41.3.8. Resumo criptográfico do SB;
 - 41.3.9. Versão do SB;
 - 41.3.10. Falhas de atualização;

41.3.11. CNPJ do fabricante do DAF;

41.3.12. Modelo DAF.

2.4.8 Requisitos do *software* básico

42. O **SB** DEVE ser executado somente após o resultado positivo da verificação de integridade executada pelo *bootloader*.
43. DEVE ser armazenado na região mutável (veja [Subseção 2.4.4](#)).
44. DEVE implementar o comportamento da máquina de estado para os estados OPERAÇÃO e seus subestados (veja [Seção 2.2](#)).
45. DEVE ser implementado de acordo com o [Capítulo 4](#), [Capítulo 5](#) e [Capítulo 6](#).
46. A versão do **SB** DEVE ser representada na forma de um número inteiro crescente.

2.4.9 Requisitos para atualização do **SB**

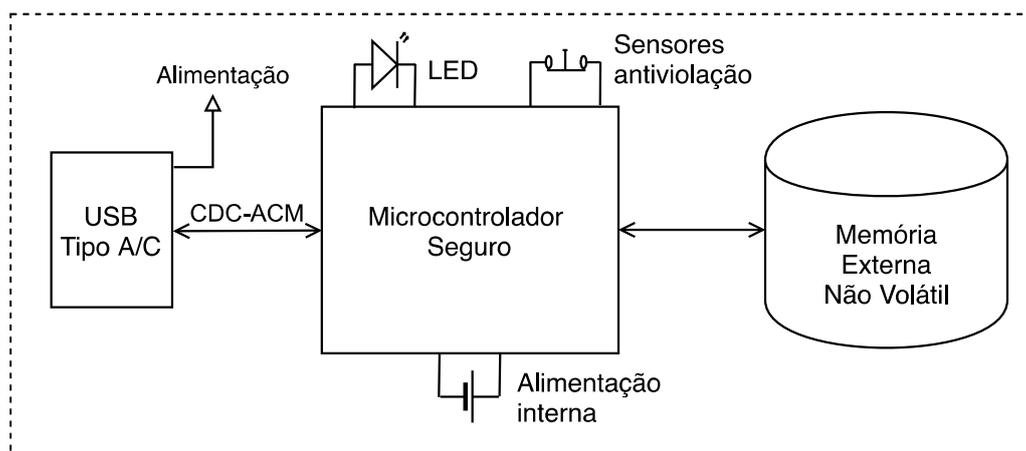
47. O *Software Básico Candidato* DEVE conter o $maxDFe$ se exigido pela SEF.
48. A SEF DEVE concatenar a versão e o código binário do *Software Básico Candidato*, obrigatoriamente nessa ordem, e gerar uma *assinatura digital* sobre o resultado.
 - 48.1. A assinatura da SEF DEVE ser gerada com a chave privada da SEF, par da chave pública contida no certificado digital inserido no DAF.
49. O fabricante do DAF DEVE concatenar a versão e o código binário do *Software Básico Candidato*, obrigatoriamente nessa ordem, e gerar uma *assinatura digital* sobre o resultado.
 - 49.1. A assinatura do fabricante DEVE ser gerada com a *chave de ateste* do DAF.
50. A imagem do **SBC** para o DAF DEVE conter:
 - 50.1. O resumo criptográfico gerado sobre o código binário do SBC;
 - 50.2. A versão do SBC;
 - 50.3. O código binário do SBC;
 - 50.4. A assinatura da SEF (veja [Item 48.](#));
 - 50.5. A assinatura do fabricante do DAF (veja [Item 49.](#)).

3 Organização do DAF

Neste capítulo será apresentada a organização do **Dispositivo Autorizador Fiscal**, ou seja, uma visão mais estrutural e detalhada da implementação da arquitetura proposta no **Capítulo 2**. Serão apresentando os componentes de *hardware* com detalhamento das interligações e os requisitos para manutenção das prerrogativas de segurança.

Na **Figura 3.1** são apresentados os componentes do DAF, os quais são: microcontrolador seguro; memória externa (opcional); fonte de alimentação externa e interna; gabinete e sistema antiviolação; componente de sinalização (**LED**); e interface de comunicação.

Figura 3.1: Organização do DAF com os componentes e interligações



Nas próximas seções serão descritos cada um dos componentes e a composição estrutural do DAF. A lista de requisitos é contínua desde o **Capítulo 2** para facilitar a referência da especificação, implementação e homologação do **DAF**.

3.1 Microcontrolador seguro

51. O microcontrolador DEVE possuir mecanismos que possibilitem a implementação do *bootloader* seguro para verificação de autenticidade e de integridade do **SB** (veja **Subseção 2.4.6**).
52. DEVE ser afixado na placa sem soquete ou conector.
53. DEVE possuir um **TRNG**.
54. DEVE possuir os mecanismos necessários para implementar o sistema antiviolação (veja **Seção 3.5**).

3.2 Memória externa não volátil

55. A organização PODE contar com um *chip* externo ao microcontrolador seguro de memória não volátil. Nesse caso, ele DEVE seguir os seguintes requisitos:

55.1. DEVE ser afixado à placa sem uso de soquete ou conector;

55.2. DEVE estar completamente protegido pelo sistema de blindagem (veja [Seção 3.5](#)).

3.3 Organização das memórias

A arquitetura de memória foi apresentada no [Capítulo 2](#). Abaixo os requisitos da organização considerando os componentes estruturais.

56. As seguintes regiões e partições de memória DEVEM estar contidas no mesmo circuito integrado do microcontrolador seguro:

56.1. Memória de dados (RAM);

56.2. Memória imutável (veja [Subseção 2.4.3](#));

56.3. Memória protegida (veja [Subseção 2.4.5](#));

56.4. Partição do SB (veja [Item 25](#)).

57. As seguintes partições PODEM ser implementadas na memória externa (veja [Seção 3.2](#)) ou DEVEM estar contidas no circuito integrado do microcontrolador seguro.

57.1. A partição MT (veja [Item 24](#));

57.2. A partição de atualização (veja [Subseção 2.4.4](#)).

3.4 Alimentação

58. O DAF DEVE ser energizado exclusivamente pelo conector USB para a sua operação normal.

59. O DAF DEVE possuir fonte interna de energia, capaz de alimentar o sistema antivolação enquanto não estiver ligado a uma porta USB, com as seguintes características:

59.1. A duração da fonte interna de energia DEVE ser de pelo menos 5 anos com equipamento desligado e de 10 anos com equipamento ligado por pelo menos 40 h por semana;

59.2. A fonte interna de energia NÃO DEVE ser passível de substituição. (veja [Item 60.3](#) da [Seção 3.5](#));

3.5 Gabinete e sistema antivolação

60. O gabinete do DAF DEVE possuir as seguintes características:

60.1. Ser blindado, isto é, ser composto por uma malha ativa de proteção dinâmica que cubra todos os componentes internos;

60.2. Ser opaco;

- 60.3. Sem encaixes e parafusos de maneira a evitar que o DAF seja aberto e depois fechado sem deixar vestígios desta abertura. Assim também impossibilitando a abertura para qualquer tipo de manutenção.
61. O sistema antivolação DEVE possuir as seguintes características:
- 61.1. Possuir sensoriamento sobre a malha ativa de proteção;
 - 61.2. Possuir sensores de temperatura, tensão e *clock*;
 - 61.3. Estar ativo com alimentação principal (USB) ou secundária (veja [Seção 3.4](#));
 - 61.4. Reagir imediatamente ao ser detectada qualquer violação.
62. O sistema antivolação DEVE disparar nos seguintes casos:
- 62.1. Abertura do gabinete;
 - 62.2. Objetos com diâmetro igual ou maior que 0,4 mm furem a malha de proteção dos componentes internos;
 - 62.3. Se pelo menos uma das seguintes condições ocorrer:
 - 62.3.1. Temperatura estiver fora do valor normal de operação da região de memória protegida;
 - 62.3.2. Tensão da fonte de energia interna estiver fora do valor normal de operação.
63. Ao ser identificada uma violação, o DAF DEVE imediatamente:
- 63.1. Apagar o material criptográfico sensível (veja [Subseção 2.4.5](#));
 - 63.2. Acionar o estado INUTILIZADO (veja [Seção 2.2](#)) e a partir disso só permitir as funcionalidades previstas para esse estado (veja [Subseção 2.4.7](#)).
64. Os únicos componentes do DAF considerados externos são:
- 64.1. Conector (plugue) USB (veja [Seção 3.6](#));
 - 64.2. LED de sinalização (veja [Seção 3.7](#)) sem a exposição dos terminais.
65. Qualquer outro componente do DAF não listado no [Item 64](#). é considerado um componente interno.

3.6 Interface de comunicação

66. O DAF DEVE possuir exclusivamente um conector (plugue) **USB-A** ou **USB-C** que permitirá tanto a alimentação do DAF quanto a troca de dados com o **PAF**.
67. DEVE implementar no mínimo a especificação USB 1.1 *Full Speed*.
68. DEVE ser somente do tipo dispositivo (*device*) e emular uma porta serial virtual por meio da subclasse *Abstract Control Model (ACM)* da classe **USB-CDC** e sem a necessidade de protocolo (*Class Protocol Code=00h*), conforme apresentado em [USB-IF \(2010, 2007\)](#).
69. O DAF PODE operar a partir da instalação de *drivers* proprietários para o funcionamento junto ao **PAF**.

- 69.1. Os *drivers* proprietários NÃO DEVEM influenciar no funcionamento de *drivers* proprietários de outros fabricantes ou dos sistemas operacionais.
70. O campo *iProduct* do *device descriptor* do dispositivo USB DEVE conter um índice referente a um *string descriptor* cujo valor seja: “DAF-SC”.
71. A comunicação do DAF com o PAF DEVE ocorrer exclusivamente com o protocolo definido no [Capítulo 6](#).

3.7 Sinalização

72. O DAF DEVE conter apenas um [Diodo Emissor de Luz \(LED\)](#), capaz de emitir três cores distintas (vermelho, verde e âmbar) para informação visual sobre seu estado atual, conforme apresentado na [Tabela 3.1](#).

Tabela 3.1: Sinalização visual referente aos estados do DAF

Estado	Cor	Padrão
BOOTLOADER	âmbar	contínuo
BLOQUEADO	âmbar	piscando
INATIVO	verde	piscando
PRONTO	verde	contínuo
INUTILIZADO	vermelho	piscando

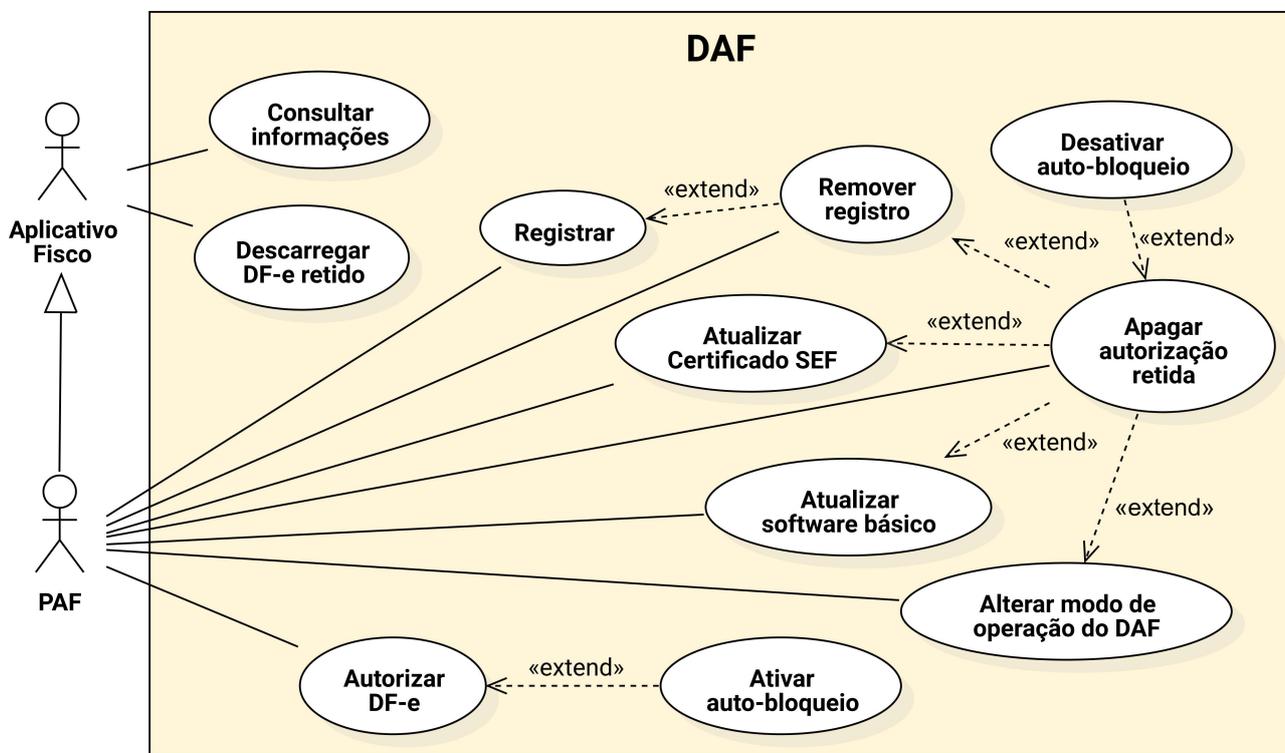
4 Software Básico

Este capítulo define os casos de uso do *Software Básico (SB)* que precisam ser implementados a fim de disponibilizar todas as funcionalidades esperadas pelo PAF e aplicativo do Fisco. O SB é responsável pelos casos de uso e o comportamento dos estados INATIVO, PRONTO e BLOQUEADO (veja Tabela 4.1 e Figura 2.2).

4.1 Cenários de uso

Nessa seção são apresentadas todas as funcionalidades que deverão ser ofertadas pelo DAF por meio de cenários de uso. Na Figura 4.1 é ilustrado um diagrama de casos de uso UML com as funcionalidades que o DAF deverá prover e que poderão ser usadas pelo PAF e pelo fiscal da SEF, quando esse vier a fazer uma visita *in loco* ao contribuinte.

Figura 4.1: Diagrama de caso de uso do DAF



1. **Alterar modo de operação do DAF (UC-4.1)** - Para configurar o modo de operação do DAF para o modo 1 DAF por PDV ou para o modo 1 DAF compartilhado por vários PDVs.
2. **Apagar autorização retida (UC-4.2)** - Para remover da MT uma autorização gerada pelo DAF

e que fora processada pela SEF;

3. **Ativar auto-bloqueio (UC-4.3)** - Estende o comportamento do caso de uso *Autorizar DF-e*, com o intuito de não permitir que o DAF faça autorização de novos documentos até que os documentos contidos em sua MT sejam processados pela SEF;
4. **Atualizar certificado SEF (UC-4.4)** - Para atualizar certificado digital da SEF armazenado no DAF;
5. **Atualizar software básico (UC-4.5)** - Para atualizar o SB do DAF;
6. **Autorizar DF-e (UC-4.6)** - Para solicitar autorização sobre um Documento Fiscal Eletrônico (DF-e) que será encaminhado à SEFAZ;
7. **Consultar informações (UC-4.7)** - Para obter informações como versão do SB, resumo criptográfico sobre o SB, Identificador único do DAF (IdDAF), modelo, CNPJ do fabricante, valor atual do contador monotônico, identificadores dos documentos retidos na MT, certificado digital da SEF armazenado, estado atual do DAF e o modo de operação do DAF;
8. **Desativar auto-bloqueio (UC-4.8)** - Estende o comportamento do caso de uso *Apagar autorização retida* para desbloquear o DAF que fora bloqueado automaticamente pelo caso de uso *Ativar auto-bloqueio*;
9. **Descarregar DF-e retido (UC-4.9)** - Para obter a autorização retida de um DF-e, o XML com as informações essenciais deste DF-e e o resumo criptográfico gerado sobre o XML do DF-e completo;
10. **Registrar (UC-4.10)** - Para registrar um DAF junto à SEF;
11. **Remover registro (UC-4.11)** - Para remover as informações de registro do DAF junto à SEF;

4.2 Descrição dos casos de uso do DAF

Nessa seção serão apresentadas as descrições de casos de uso presentes na Figura 4.1.

UC-4.1: Alterar modo de operação do DAF

Resumo Esse caso de uso descreve as etapas para alterar o modo de operação do DAF. Os modos possíveis são: 1 DAF por PDV; ou 1 DAF compartilhado por vários PDVs.

Ator primário PAF

Pré-condições DAF deve estar no estado PRONTO (veja Seção 2.2)

Fluxo principal

1. O PAF encaminha o documento recebido da SEF (veja descrição no comando na Subsubseção 6.1.2.12)
2. O DAF verifica se está no estado PRONTO
3. O DAF verifica se o pedido foi formado adequadamente
4. O DAF verifica se existem autorizações retidas em sua memória de trabalho (veja Caso de Uso UC-4.2)

5. O DAF verifica a integridade e autenticidade da mensagem recebida por meio de uma função HMAC que teve como chave a [chave SEF](#)
6. O DAF gera um documento de solicitação de alteração do modo de operação do DAF, o qual contém seu [IdDAF](#), o atual valor de seu [contador monotônico](#) e o *nonce* recebido pela SEF
7. O DAF retorna para o PAF um documento estruturado, cuja integridade e autenticidade é garantida por meio de uma função HMAC que teve como chave a [chave SEF](#), contendo o documento gerado no passo anterior
8. O PAF encaminha ao DAF o documento recebido da SEF, o qual contém a autorização para fazer a alteração do modo de operação do DAF (veja descrição da mensagem na [Subsubseção 6.1.2.13](#))
9. O DAF verifica se o pedido foi formado adequadamente e se o documento encaminhado contém o novo modo de operação do DAF
10. O DAF verifica a integridade e autenticidade da mensagem recebida por meio de uma função HMAC que teve como chave a [chave SEF](#)
11. O DAF altera seu modo de operação do DAF
12. O DAF retorna ao PAF uma mensagem informando que o modo de operação do DAF foi alterado com sucesso

Fluxo de exceção: DAF em estado incorreto

1. O DAF retorna para o PAF uma mensagem de erro informando que não está no estado correto (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: Autorizações retidas

1. O DAF retorna para o PAF uma mensagem de erro informando que existem autorizações retidas em sua memória de trabalho (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: HMAC recebido diferente do HMAC gerado pelo DAF

1. O DAF retorna para o PAF uma mensagem de erro informando que não houve correspondência entre o HMAC recebido e o HMAC gerado pelo DAF (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: Pedido mal formado

1. O DAF retorna para o PAF uma mensagem de erro informando que o pedido foi mal formado (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: DAF não recebe mensagem esperada dentro de 120 segundos

1. O DAF aborta o caso de uso em execução

Fluxo de exceção: DAF recebe mensagem que não faz parte do caso de uso em execução

1. O DAF retorna para o PAF uma mensagem de erro informando que o pedido foi mal formado (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: DAF recebe mensagem para abortar o caso de uso em execução

1. O DAF aborta o caso de uso em execução e retorna ao PAF mensagem indicando sucesso na operação

UC-4.2: Apagar autorização retida

Resumo Esse caso de uso descreve as etapas para apagar uma autorização retida na **MT** do DAF.

Ator primário PAF

Pré-condições DAF deve estar no estado PRONTO ou BLOQUEADO (veja [Seção 2.2](#))

Fluxo principal

1. PAF encaminha autorização processada pela SEF para remoção de autorização retida no DAF (veja descrição da mensagem na [Subsubseção 6.1.2.5](#))
2. O DAF verifica se está no estado PRONTO ou BLOQUEADO
3. O DAF verifica se o pedido foi formado adequadamente
4. O DAF verifica se o **Identificador único da autorização DAF (idAut)** está armazenado em sua MT
5. O DAF gera um HMAC tendo como chave a **chave SEF** e como mensagem o **idAut** e verifica se há correspondência com o HMAC recebido do PAF
6. O DAF apaga a autorização retida de sua MT
7. O DAF verifica se está no estado BLOQUEADO (veja [Caso de Uso UC-4.8](#))
8. O DAF retorna para o PAF uma mensagem informando que a autorização foi removida com sucesso

Fluxo de exceção: DAF em estado incorreto

1. O DAF retorna para o PAF uma mensagem de erro informando que não está no estado correto (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: Pedido mal formado

1. O DAF retorna para o PAF uma mensagem de erro informando que o pedido foi mal formado (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: HMAC recebido diferente do HMAC gerado pelo DAF

1. O DAF retorna para o PAF uma mensagem de erro informando que não houve correspondência entre o HMAC recebido e o HMAC gerado pelo DAF (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: Autorização não encontrada

1. O DAF retorna para o PAF uma mensagem de erro informando que o **idAut** não foi encontrado (veja descrição do erro na [Tabela 6.2](#))

UC-4.3: Ativar auto-bloqueio

Resumo Esse caso de uso descreve as etapas para ativar o auto-bloqueio do DAF, para não permitir que o DAF emita novas autorizações até que alguns dos documentos retidos em sua MT sejam processados pela SEF.

Pré-condições DAF deve estar no estado de PRONTO (veja [Seção 2.2](#))

Pós-condições DAF deve terminar no estado BLOQUEADO

Fluxo principal

1. O DAF verifica que o limite de autorizações retidas em sua MT foi atingido
2. O DAF ativa seu auto-bloqueio, alterando seu estado para BLOQUEADO

UC-4.4: Atualizar certificado da SEF

Resumo Esse caso de uso descreve as etapas para atualizar certificado digital da SEF armazenado no DAF.

Ator primário PAF

Pré-condições DAF deve estar no estado PRONTO ou INATIVO (veja [Seção 2.2](#))

Pós-condições DAF deve terminar no estado PRONTO ou INATIVO

Fluxo principal

1. O PAF transfere para o DAF o novo certificado digital da SEF (veja descrição da mensagem na [Subsubseção 6.1.2.10](#))
2. O DAF verifica se está no estado PRONTO ou INATIVO
3. O DAF verifica se o pedido foi formado adequadamente
4. O DAF verifica se existem autorizações retidas em sua MT (veja [Caso de Uso UC-4.2](#))
5. O DAF verifica se o novo certificado foi assinado com a [chave privada](#) correspondente à [chave pública](#) presente no atual [certificado digital da SEF](#) que o DAF possui
6. O DAF substitui, em sua memória, o atual [certificado digital da SEF](#) pelo novo certificado recebido
7. O DAF informa ao PAF que a atualização de certificado digital foi bem sucedida

Fluxo de exceção: DAF em estado incorreto

1. O DAF retorna para o PAF uma mensagem de erro informando que não está no estado correto (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: Pedido mal formado

1. O DAF retorna para o PAF uma mensagem de erro informando que o pedido foi mal formado (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: Autorizações retidas

1. O DAF retorna para o PAF uma mensagem de erro informando que existem autorizações retidas em sua [MT](#) (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: Assinatura da SEF é inválida

1. O DAF retorna para o PAF uma mensagem de erro informando que a assinatura é inválida (veja descrição do erro na [Tabela 6.2](#))

UC-4.5: Atualizar Software Básico

Resumo Esse caso de uso descreve as etapas para atualizar o [SB](#) do [DAF](#).

Ator primário [PAF](#)

Pré-condições [DAF](#) deve estar no estado PRONTO ou INATIVO (veja [Seção 2.2](#))

Fluxo principal

1. O [PAF](#) informa ao [DAF](#) que iniciará o processo de atualização de [SB](#) (veja descrição da mensagem na [Subsubseção 6.1.2.9](#))
2. O [DAF](#) verifica se está no estado PRONTO ou INATIVO
3. O [DAF](#) verifica se possui autorizações retidas em sua [MT](#) (veja [Caso de Uso UC-4.2](#))
4. O [DAF](#) responde ao [PAF](#) que está pronto para a atualização de [SB](#)
5. O [PAF](#) transfere para o [DAF](#) o [SB](#) candidato (veja descrição do comando na [Subseção 6.2.4](#))
6. O [DAF](#) armazena o [SB](#) candidato na partição de atualização (veja [Capítulo 2](#))
7. O [DAF](#) verifica se a versão do [SB](#) candidato é superior à versão instalada
8. O [DAF](#) verifica se o [SB](#) candidato foi assinado com a [chave de ateste](#) do mesmo
9. O [DAF](#) verifica a integridade e autenticidade do [SB](#) recebido a partir da assinatura gerada pela [SEF](#)
10. O [DAF](#) informa ao [PAF](#) que o [SB](#) candidato é válido
11. O [DAF](#) é reiniciado automaticamente

Fluxo de exceção: DAF em estado incorreto

1. O [DAF](#) retorna para o [PAF](#) uma mensagem de erro informando que não está no estado correto (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: Autorizações retidas

1. O [DAF](#) retorna para o [PAF](#) uma mensagem de erro informando que existem autorizações retidas em sua [MT](#) (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: Versão do SB candidato é inferior a versão do SB atual

1. O DAF apaga a partição de atualização (veja [Capítulo 2](#))
2. O DAF retorna para o PAF uma mensagem de erro informando que a versão do SB recebido é inferior a versão armazenada (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: Assinatura da SEF sobre o SB candidato é inválida

1. O DAF apaga a partição de atualização (veja [Capítulo 2](#))
2. O DAF retorna para o PAF uma mensagem de erro informando que a assinatura é inválida (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: Modelo de DAF do SB candidato não é igual ao do DAF em questão

1. O DAF apaga a partição de atualização (veja [Capítulo 2](#))
2. O DAF retorna para o PAF uma mensagem de erro informando que o modelo de DAF do SB candidato é diferente do modelo do DAF em questão (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: DAF não recebe mensagem esperada dentro de 120 segundos

1. O DAF aborta o caso de uso em execução

Fluxo de exceção: DAF recebe mensagem que não faz parte do caso de uso em execução

1. O DAF retorna para o PAF uma mensagem de erro informando que o pedido foi mal formado (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: DAF recebe mensagem para abortar o caso de uso em execução

1. O DAF aborta o caso de uso em execução e retorna ao PAF mensagem indicando sucesso na operação

UC-4.6: Autorizar DF-e

Resumo Esse caso de uso descreve as etapas para autorizar um [DF-e](#) utilizando o DAF.

Ator primário PAF

Pré-condições DAF deve estar no estado PRONTO (veja [Seção 2.2](#))

Fluxo principal

1. O PAF solicita ao DAF um *nonce* para autenticação (veja descrição da mensagem na [Subsubseção 6.1.2.3](#))
2. O DAF gera um *nonce*, persiste em sua memória RAM e o retorna ao PAF
3. O PAF solicita ao DAF a emissão de autorização sobre um DF-e e envia o conjunto de informações essenciais do DF-e (veja [Subseção 5.2.1](#)), o **resumo criptográfico do XML** completo do DF-e, o **Identificador único do PDV (IdPDV)** e código de autenticação do PAF (veja descrição da mensagem na [Subsubseção 6.1.2.4](#))
 - Código de autenticação do PAF consiste na saída de uma **função hash criptográfica HMAC** (KRAWCZYK; BELLARE; CANETTI, 1997) que teve como chave a **chave PAF** e

como mensagem o *nonce* recebido do DAF concatenado com o [resumo criptográfico](#) do XML completo do DF-e

4. O DAF verifica se está no estado PRONTO
5. O DAF verifica se o pedido foi formado adequadamente
6. O DAF calcula o HMAC com a mesma chave e mensagem usadas pelo PAF e verifica a correspondência com o HMAC recebido, validando o código de autenticação do PAF
7. O DAF, a partir do resumo criptográfico gerado sobre o XML completo do DF-e, verifica se não possui autorização retida para o DF-e em questão em sua [MT](#)
8. O DAF incrementa seu [contador monotônico](#)
9. O DAF gera um documento estruturado contendo: o [IdDAF](#), a versão atual do [SB](#), o seu [modo de operação do DAF](#), o [IdPDV](#), o atual valor de seu [contador monotônico](#) e o [Identificador único da autorização DAF \(idAut\)](#). O [idAut](#) consiste na saída de uma função [HMAC](#) que teve como chave a [chave SEF](#) e como mensagem as seguintes informações concatenadas: o atual valor de seu [contador monotônico](#), o fragmento XML com as informações essenciais do DF-e e o [resumo criptográfico](#) sobre o XML completo do DF-e em questão
10. O DAF associa o documento gerado com o documento XML de informações essenciais do DF-e e o resumo criptográfico sobre o XML completo do DF-e, persistindo-os em sua [MT](#)
11. O DAF verifica se o limite de autorizações retidas em sua [MT](#) foi atingido
12. O DAF retorna para o PAF um documento estruturado, cuja integridade e autenticidade é garantida por meio de uma função HMAC que teve como chave a [chave SEF](#), contendo o documento gerado nos passos anteriores

Fluxo alternativo: Ativar auto-bloqueio

1. O DAF verifica que o limite de autorizações retidas em sua [MT](#) foi atingido
2. O DAF altera seu estado para BLOQUEADO (veja [Caso de Uso UC-4.3](#))

Fluxo de exceção: DAF em estado incorreto

1. O DAF retorna para o PAF uma mensagem de erro informando que não está no estado correto (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: PAF não autenticado

1. O DAF retorna para o PAF uma mensagem de erro informando que o PAF não foi autenticado, pois o *nonce* é inválido (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: Pedido mal formado

1. O DAF retorna para o PAF uma mensagem de erro informando que o pedido foi mal formado (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: DAF não recebe mensagem esperada dentro de 120 segundos

1. O DAF aborta o caso de uso em execução

Fluxo de exceção: DAF recebe mensagem que não faz parte do caso de uso em execução

1. O DAF retorna para o PAF uma mensagem de erro informando que o pedido foi mal formado (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: DAF recebe mensagem para abortar o caso de uso em execução

1. O DAF aborta o caso de uso em execução e retorna ao PAF mensagem indicando sucesso na operação

UC-4.7: Consultar informações

Resumo Esse caso de uso descreve as etapas para o PAF obter informações como versão do SB, [resumo criptográfico](#) sobre o SB, [IdDAF](#), modelo, CNPJ do fabricante, valor atual do contador monotônico, [certificado digital da SEF](#) armazenado, estado do DAF, identificadores dos documentos retidos na [MT](#) e o [modo de operação do DAF](#).

Ator primário PAF ou Aplicativo Fisco

Pré-condições DAF deve estar no estado PRONTO, INATIVO ou BLOQUEADO (veja [Seção 2.2](#))

Fluxo principal

1. O PAF, ou Aplicativo Fisco, solicita ao DAF suas informações (veja descrição da mensagem na [Subsubseção 6.1.2.8](#))
2. O DAF retorna para o PAF, ou Aplicativo Fisco, o documento estruturado com suas informações

UC-4.8: Desativar auto-bloqueio

Resumo Esse caso de uso descreve as etapas para desbloquear o DAF que fora bloqueado automaticamente pelo [Caso de Uso UC-4.3](#).

Pré-condições DAF deve estar no estado de BLOQUEADO (veja [Seção 2.2](#))

Fluxo principal

1. O DAF verifica se está no estado BLOQUEADO
2. O DAF verifica que o limite de autorizações retidas em sua MT não foi atingido
3. O DAF altera seu estado para PRONTO

UC-4.9: Descarregar DF-e retido

Resumo Esse caso de uso descreve as etapas para obter a autorização retida de um [DF-e](#), o XML com as informações essenciais deste DF-e e o [resumo criptográfico](#) gerado sobre o XML do DF-e completo.

Ator primário PAF ou Aplicativo Fisco

Pré-condições DAF deve estar no estado PRONTO (veja [Seção 2.2](#))

Fluxo principal

1. O PAF, ou Aplicativo Fisco, informa ao DAF o **idAut** (veja descrição da mensagem na [Subsubseção 6.1.2.11](#))
2. O DAF verifica se o pedido foi formado adequadamente
3. O DAF verifica se o **idAut** solicitado está armazenado em sua MT
4. O DAF retorna para o PAF, ou Aplicativo Fisco, o conjunto de informações essenciais, o **resumo criptográfico** e a autorização do **DF-e**

Fluxo de exceção: Pedido mal formado

1. O DAF retorna para o PAF, ou Aplicativo Fisco, uma mensagem de erro informando que o pedido foi mal formado (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: Autorização não encontrada

1. O DAF retorna para o PAF, ou Aplicativo Fisco, uma mensagem de erro informando que o **idAut** não foi encontrado (veja descrição do erro na [Tabela 6.2](#))

UC-4.10: Registrar

Resumo Esse caso de uso descreve as etapas para registrar um **DAF** junto à **SEF**. Esse procedimento é obrigatório para que se possa usar as demais funcionalidades do DAF junto à SEF.

Ator primário PAF

Pré-condições DAF deve estar no estado INATIVO (veja [Seção 2.2](#))

Pós-condições DAF deve terminar no estado PRONTO

Fluxo principal

1. O PAF encaminha um desafio de registro recebido da SEF (veja descrição da mensagem na [Subsubseção 6.1.2.1](#))
2. O DAF verifica se está no estado INATIVO
3. O DAF verifica se o pedido foi formado adequadamente
4. O DAF verifica se a mensagem foi assinada pela SEF
5. O DAF gera um par de chaves criptográficas
6. O DAF armazena a **chave privada do DAF**
7. O DAF gera um documento contendo o atual valor de seu **contador monotônico**, o **IdDAF**, sua chave pública, e o **nonce** fornecido pela SEF. Esse documento é então assinado com sua chave privada, depois assinado com a **chave de ateste** e por fim, encaminhado ao PAF
8. O PAF encaminha a mensagem de confirmação registro enviada pela SEF, contendo a **chave SEF** (cifrada com a chave pública do DAF), a **chave PAF** e o modo de operação do DAF (veja descrição da mensagem na [Subsubseção 6.1.2.2](#))
9. O DAF verifica se o pedido foi formado adequadamente

10. O DAF verifica se a mensagem foi assinada pela SEF
11. O DAF armazena a [chave PAF](#) e decifra e armazena a [chave SEF](#)
12. O DAF altera seu estado para PRONTO
13. O DAF retorna para o PAF uma mensagem informando que foi registrado com sucesso

Fluxo de exceção: DAF em estado incorreto

1. O DAF retorna para o PAF uma mensagem de erro informando que não está no estado correto (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: Assinatura da SEF é inválida

1. O DAF retorna para o PAF uma mensagem de erro informando que a assinatura é inválida (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: Pedido mal formado

1. O DAF retorna para o PAF uma mensagem de erro informando que o pedido foi mal formado (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: DAF não recebe mensagem esperada dentro de 120 segundos

1. O DAF aborta o caso de uso em execução

Fluxo de exceção: DAF recebe mensagem que não faz parte do caso de uso em execução

1. O DAF retorna para o PAF uma mensagem de erro informando que o pedido foi mal formado (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: DAF recebe mensagem para abortar o caso de uso em execução

1. O DAF aborta o caso de uso em execução e retorna ao PAF mensagem indicando sucesso na operação

UC-4.11: Remover registro

Resumo Esse caso de uso descreve as etapas para remover o registro do [DAF](#) junto à [SEF](#).

Ator primário [PAF](#)

Pré-condições DAF deve estar no estado PRONTO (veja [Seção 2.2](#))

Pós-condições DAF deve terminar no estado INATIVO

Fluxo principal

1. O PAF encaminha o documento recebido da SEF (veja descrição no comando na [Subsubseção 6.1.2.6](#))
2. O DAF verifica se está no estado PRONTO
3. O DAF verifica se o pedido foi formado adequadamente
4. O DAF verifica se existem autorizações retidas em sua memória de trabalho (veja [Caso de Uso UC-4.2](#))
5. O DAF verifica se a mensagem foi assinada pela SEF

6. O DAF gera um documento de solicitação de remoção de registro o qual contém seu **IdDAF**, o atual valor de seu **contador monotônico** e o *nonce* recebido pela SEF. Esse documento é então assinado com a **chave privada do DAF** e encaminhado ao PAF
7. O PAF encaminha o documento recebido da SEF com a autorização para remoção de registro (veja descrição da mensagem na [Subsubseção 6.1.2.7](#))
8. O DAF verifica se o pedido foi formado adequadamente e se o documento encaminhado contém a cadeia de caracteres `REMOVED`
9. O DAF verifica se a mensagem foi assinada pela SEF
10. O DAF, em uma **transação atômica**, apaga de sua memória segura a **chave privada do DAF**, a **chave SEF** e a **chave PAF**
11. O DAF altera seu estado para INATIVO
12. O DAF retorna ao PAF uma mensagem informando que o registro foi removido com sucesso

Fluxo de exceção: DAF em estado incorreto

1. O DAF retorna para o PAF uma mensagem de erro informando que não está no estado correto (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: Autorizações retidas

1. O DAF retorna para o PAF uma mensagem de erro informando que existem autorizações retidas em sua memória de trabalho (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: Assinatura da SEF é inválida

1. O DAF retorna para o PAF uma mensagem de erro informando que a assinatura é inválida (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: Pedido mal formado

1. O DAF retorna para o PAF uma mensagem de erro informando que o pedido foi mal formado (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: DAF não recebe mensagem esperada dentro de 120 segundos

1. O DAF aborta o caso de uso em execução

Fluxo de exceção: DAF recebe mensagem que não faz parte do caso de uso em execução

1. O DAF retorna para o PAF uma mensagem de erro informando que o pedido foi mal formado (veja descrição do erro na [Tabela 6.2](#))

Fluxo de exceção: DAF recebe mensagem para abortar o caso de uso em execução

1. O DAF aborta o caso de uso em execução e retorna ao PAF mensagem indicando sucesso na operação

4.3 Classificação dos casos de uso

A Tabela 4.1 relaciona os casos de uso disponíveis em cada subestado do estado OPERAÇÃO (veja Figura 2.2).

Tabela 4.1: Casos de uso disponíveis em cada subestado do estado OPERAÇÃO

Caso de uso	Subestados OPERAÇÃO		
	INATIVO	PRONTO	BLOQUEADO
Alterar modo de operação do DAF		☑	
Apagar autorização retida		☑	☑
Ativar auto-bloqueio		☑	
Atualizar certificado SEF	☑	☑	
Atualizar Software Básico	☑	☑	
Autorizar DF-e		☑	
Consultar informações	☑	☑	☑
Desativar auto-bloqueio			☑
Descarregar DF-e retido		☑	☑
Registrar	☑		
Remover registro		☑	

5 Processos operacionais com o DAF

Nesse capítulo são apresentados todos os processos operacionais com o DAF e as interações com o PAF e com a SEF. Para os processos apresentados nesse capítulo foram assumidas as seguintes premissas:

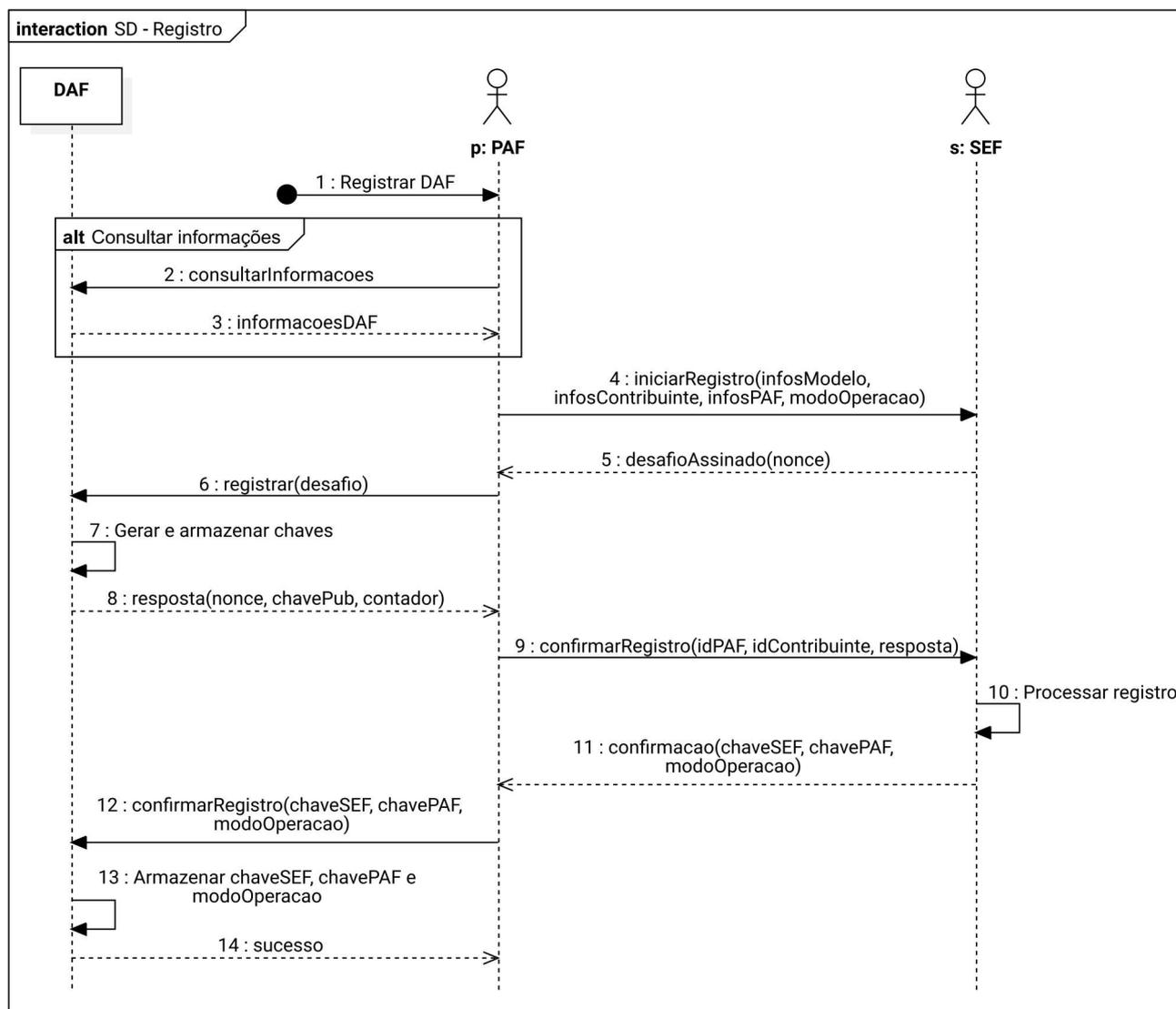
1. Contribuinte possui registro junto à SEF e possui e-CNPJ válido;
2. PAF possui registro junto à SEF e tem o Código de Segurança do Responsável Técnico (CSRT) (ENCAT, 2019c) associado a esse;
3. O desenvolvedor do PAF gerou um Identificador único do PAF (IdPAF) para o contribuinte;
 - 3.1. O IdPAF consiste na saída de uma função *hash* criptográfica HMAC-SHA256 (KRAWCZYK; BELLARE; CANETTI, 1997), representada em Base64URL (JOSEFSSON, 2006), que teve como chave o CSRT e como mensagem o CNPJ do contribuinte, representado no formato XX.XXX.XXX/YYYY-ZZ;
4. O desenvolvedor do PAF entregou ao contribuinte o IdPAF, o idCSRT e seu CNPJ;
5. DAF está fisicamente conectado no mesmo computador onde o PAF está sendo executado ou no PAF servidor, quando o DAF for compartilhado por vários PDVs;
6. DAF está certificado pela SEF;
7. Toda comunicação entre PAF e SEF é feita sobre canais de comunicação seguros [p. ex. *Transport Layer Security* (TLS) (RESCORLA, 2018)].

5.1 Registro do DAF junto à SEF

Na Figura 5.1 é ilustrado um diagrama de sequência UML que, para facilitar o entendimento, contém somente o fluxo principal para registro do DAF junto à SEF. No caso, assume-se como premissa que o DAF está no estado INATIVO (veja Seção 2.2). Fluxos alternativos e de exceção para esse processo são apresentados nos Casos de Uso UC-4.10 e UC-4.7.

1. O registro é iniciado pelo contribuinte, o qual invoca rotina específica do PAF para registro de DAF;
2. O PAF consulta informações sobre o DAF, como seu IdDAF, modelo, CNPJ do fabricante, etc (veja descrição da mensagem na Subsubseção 6.1.2.8);
3. O DAF retorna as informações solicitadas;
4. PAF envia à SEF pedido para registro de DAF (veja descrição do serviço na Subseção 8.5.1)

Figura 5.1: Diagrama de sequência do processo de registro do DAF



- 4.1. O pedido contém o **IdDAF**, o modelo e **CNPJ** do fabricante do DAF, **CNPJ** do contribuinte e informações sobre o PAF, o que inclui o **IdPAF** daquele **contribuinte**, **CNPJ** do responsável técnico do PAF, o **idCSRT** que foi usado para gerar o **IdPAF** e o **modo de operação** do DAF;
- 4.2. O pedido é assinado com o **e-CNPJ** do **contribuinte** desejado.
5. A SEF gera um **nonce** e armazena-o juntamente com as informações recebidas no pedido. Após isso, gera um desafio ao PAF, contendo o **nonce** gerado, e o assina com sua **chave privada**;
6. O PAF, ao receber o desafio da SEF, encaminha-o ao DAF (veja descrição da mensagem na [Subsubseção 6.1.2.1](#));
7. O DAF recebe o pedido e:
 - 7.1. Verifica se seu estado atual é **INATIVO** (veja [Seção 2.2](#));
 - 7.2. Verifica se o pedido foi formado adequadamente;
 - 7.3. Verifica se a assinatura da SEF sobre o desafio é válida;
 - 7.4. Gera um par de chaves criptográficas (**chave privada** e **chave pública**);

- 7.5. Armazena a *chave privada do DAF* em sua área de memória segura.
8. O DAF gera um documento contendo o atual valor de seu *contador monotônico*, o *IdDAF*, sua chave pública, e o *nonce* fornecido pela SEF. Esse documento é então assinado com sua chave privada e com a *chave de ateste* e encaminhado ao PAF;
9. O PAF encaminha a resposta do DAF à SEF juntamente com seu *IdPAF* e assina tudo isso com o *e-CNPJ* do contribuinte (veja descrição do serviço na *Subseção 8.5.2*);
10. A SEF verifica se o desafio foi atendido, validando: o valor do *nonce*; a assinatura gerada pela *chave privada do DAF*; a assinatura gerada pela *chave de ateste* e se a mesma corresponde a um modelo de DAF que já fora certificado pela SEF. Por fim, a SEF persiste o *IdPAF*, informações do contribuinte, o *IdDAF*, a chave pública do DAF, o identificador do modelo de DAF, o valor do *modo de operação do DAF* e o valor do *contador monotônico* do DAF;
11. A SEF gera um documento contendo a *chave SEF*, que fora cifrada com a chave pública do DAF; a *chave PAF*; e o *modo de operação do DAF*. Por fim, assina e encaminha esse documento ao PAF;
12. O PAF armazena a *chave PAF* e encaminha ao DAF a mensagem recebida da SEF (veja descrição da mensagem na *Subsubseção 6.1.2.2*);
13. O DAF recebe o pedido e, em uma *transação atômica*:
 - 13.1. Verifica se o pedido foi formado adequadamente;
 - 13.2. Verifica se a assinatura da SEF sobre a mensagem é válida;
 - 13.3. Decifra e armazena a *chave SEF*;
 - 13.4. Armazena a *chave PAF*;
 - 13.5. Armazena o *modo de operação do DAF*;
 - 13.6. O DAF altera seu estado para PRONTO.
14. O *DAF* retorna a mensagem de sucesso ao *PAF*, que por sua vez informa ao usuário.

Exemplos de mensagens para os comandos do DAF e serviços providos pela SEF envolvidos neste processo são apresentados na *Seção B.1*.

5.1.1 Exceções

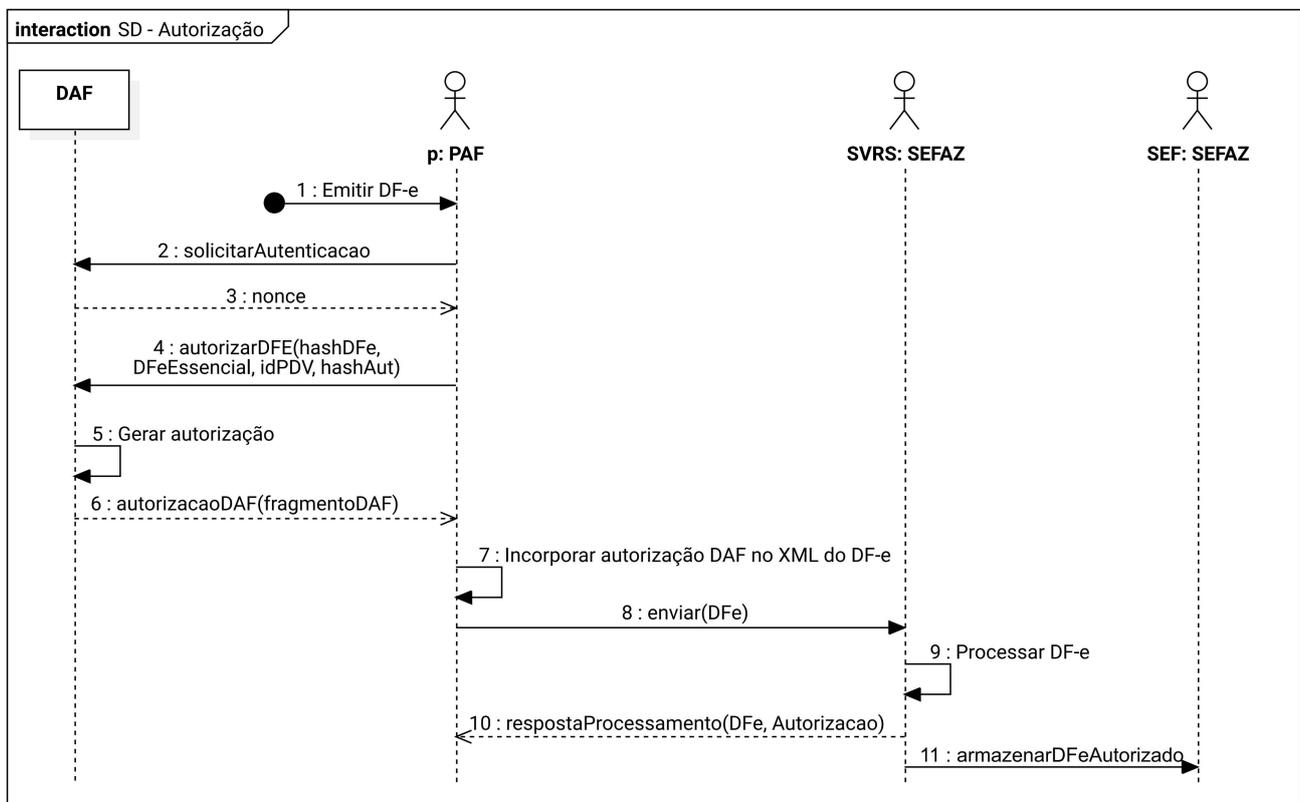
Durante o processo, o PAF é responsável pela comunicação com o DAF e a SEF. Assim, caso um destes sistemas incorram em exceção, a mensagem será tratada pelo PAF. A *Figura 5.2* ilustra o diagrama de atividade UML, especificando as exceções possíveis no processo de registro do DAF junto à SEF.

5.2 Autorização de Documentos Fiscais Eletrônicos (DF-e)

Na [Figura 5.3](#) é ilustrado um diagrama de sequência UML que, para facilitar o entendimento, contém somente o fluxo principal para emissão de um DF-e utilizando o DAF e considerando o serviço disponibilizado pela SEFAZ para autorização de documentos de modo síncrono. Fluxos alternativos e de exceção para esse processo são apresentados na [Subseção 5.2.4](#), nos Casos de Uso UC-4.6 e UC-4.3.

Uma vez que esse processo tenha terminado com sucesso, o [contribuinte](#) terá um DF-e autorizado pra uso e o DAF terá a autorização, relacionada a esse documento, retida em sua MT. Essa autorização retida deverá ser excluída posteriormente e a descrição desse processo está descrito na [Seção 5.3](#).

Figura 5.3: Diagrama de sequência do processo de autorização de um DF-e



1. A emissão do DF-e é iniciada pelo [contribuinte](#), o qual invoca a rotina específica do PAF para autorização de DF-e;
2. O PAF envia ao DAF mensagem solicitando um *nonce* (veja descrição da mensagem na [Subsubseção 6.1.2.3](#));
3. O DAF gera um *nonce*, persiste em sua memória RAM e o retorna ao PAF;
4. O PAF envia ao DAF um documento XML contendo as informações essenciais do DF-e em questão (veja [Subseção 5.2.1](#)), um [resumo criptográfico](#) (*hash*) gerado sobre o XML completo do DF-e, o *IdPDV*, e a saída de uma [função hash criptográfica HMAC-SHA256](#) que teve como chave a *chave PAF* e como mensagem o *nonce* recebido do DAF e o [resumo criptográfico](#) sobre o XML completo do DF-e, concatenados na ordem em que se apresentam (veja descrição da mensagem na [Subsubseção 6.1.2.4](#));

- 4.1. Antes de gerar o resumo criptográfico sobre o documento XML completo do DF-e, o PAF DEVE remover do documento XML em questão, os caracteres de nova linha; e os espaços em branco usados somente para facilitar a legibilidade e que sejam insignificantes para a informação que está sendo carregada;
5. O DAF recebe o pedido e, em uma **transação atômica**:
 - 5.1. Verifica se seu estado atual é PRONTO (veja [Seção 2.2](#));
 - 5.2. Verifica se o pedido foi formado adequadamente;
 - 5.3. Calcula o HMAC com a mesma chave e mensagem usadas pelo PAF e verifica a correspondência com o HMAC recebido;
 - 5.4. Verifica, a partir do resumo criptográfico gerado sobre o XML completo do DF-e, se possui autorização retida em sua **MT** para o DF-e em questão;
 - 5.5. Incrementa seu **contador monotônico**;
 - 5.6. Gera um documento estruturado contendo: o **IdDAF**, a versão atual do **SB**, o **modo de operação do DAF**, o **IdPDV**, o atual valor de seu **contador monotônico** e o **idAut**. O **idAut** consiste na representação em Base64URL de um **HMAC** que teve como chave a **chave SEF** e como mensagem as seguintes informações concatenadas na ordem em que se apresentam: o atual valor de seu **contador monotônico**, o documento XML com as informações essenciais do DF-e e o **resumo criptográfico** sobre o XML completo do DF-e em questão;
 - 5.7. Associa o documento gerado com o documento XML de informações essenciais do DF-e e com o resumo criptográfico, que fora gerado sobre o XML completo do DF-e, persistindo-os em sua **MT**;
 - 5.8. Se o limite de autorizações retidas em sua **MT** foi atingido, então passa para o estado BLOQUEADO (veja [Caso de Uso UC-4.3](#)).
6. O DAF retorna para o PAF um documento estruturado, cuja integridade e autenticidade é garantida por meio de uma função HMAC que teve como chave a **chave SEF**, contendo o documento gerado nos passos anteriores;
7. PAF incorpora no DF-e gerado anteriormente o documento enviado pelo DAF (veja [Subseção 5.2.3](#)). Por fim, assina o DF-e com o **e-CNPJ** do **contribuinte**, seguindo assim o procedimento que é posto pelo manual do contribuinte do DF-e em questão ([ENCAT, 2019a,b](#));
8. O PAF envia o DF-e para a SEFAZ e solicita a autorização, conforme é posto pelo manual do contribuinte do DF-e em questão ([ENCAT, 2019a,b](#));
9. A SEFAZ processa o pedido de autorização do DF-e, que PODE incluir a verificação da presença do fragmento gerado pelo DAF;
10. A SEFAZ retorna a resposta sobre a autorização do DF-e;
11. A SEFAZ encaminha o **DF-e** processado para à **SEF**.

Exemplos de mensagens para os comandos do DAF e serviços providos pela SEF envolvidos neste processo são apresentados na [Seção B.3](#).

5.2.1 Conjunto de informações essenciais do DF-e a ser montado pelo PAF

O PAF DEVE montar um documento XML com um conjunto de informações essenciais do DF-e que deseja obter autorização. Esse documento consiste de um subconjunto do DF-e completo e para a NFC-e DEVE conter somente os seguintes grupos que estão contidos no grupo *infNFe*, sendo esse o grupo raiz do novo documento:

- *ide* – grupo com as informações de identificação do documento;
- *total* – grupo que reúne os valores totais do documento.

Na [Tabela 5.1](#) é apresentada a estrutura do documento XML com o conjunto essencial para NFC-e. Na primeira coluna é indicada a ordem do grupo, e dos atributos de um grupo, no documento e na segunda coluna o *ID*, um código do campo de acordo com o leiaute da NFC-e ([ENCAT, 2019a](#)).

Tabela 5.1: Conjunto de informações essenciais de uma NFC-e

#	ID	Campo	Descrição
1	A01	<i>infNFe</i>	Grupo raiz do documento com informações essenciais
2	A02	<i>versao</i>	Atributo de <i>infNFe</i> com a versão do leiaute da NFC-e
3	A03	<i>ID</i>	Atributo de <i>infNFe</i> com a chave de acesso da NFC-e
4	B01	<i>ide</i>	Grupo de informações de identificação da NFC-e
5	W01	<i>total</i>	Valores totais da NFC-e

O conjunto de informações essenciais para autorização de BP-e DEVE incluir, de modo semelhante ao conjunto para NFC-e, a chave de acesso, o grupo de informações com a identificação e o grupo de informações com os valores. Na [Tabela 5.2](#) é apresentada a estrutura do documento XML com o conjunto essencial para BP-e. Na primeira coluna é indicada a ordem do grupo, e dos atributos de um grupo, no documento e na segunda coluna o *ID*, um código do campo de acordo com o leiaute da [ENCAT \(2019b\)](#).

Tabela 5.2: Conjunto de informações essenciais de um BP-e

#	ID	Campo	Descrição
1	1	<i>infBP</i>	Grupo raiz do documento com informações essenciais
2	2	<i>versao</i>	Atributo de <i>infBP</i> com a versão do leiaute do BP-e
3	3	<i>ID</i>	Atributo de <i>infBP</i> com a chave de acesso do BP-e
4	4	<i>ide</i>	Grupo de informações de identificação do BP-e
5	125	<i>imp</i>	Grupo com informações relativas aos impostos

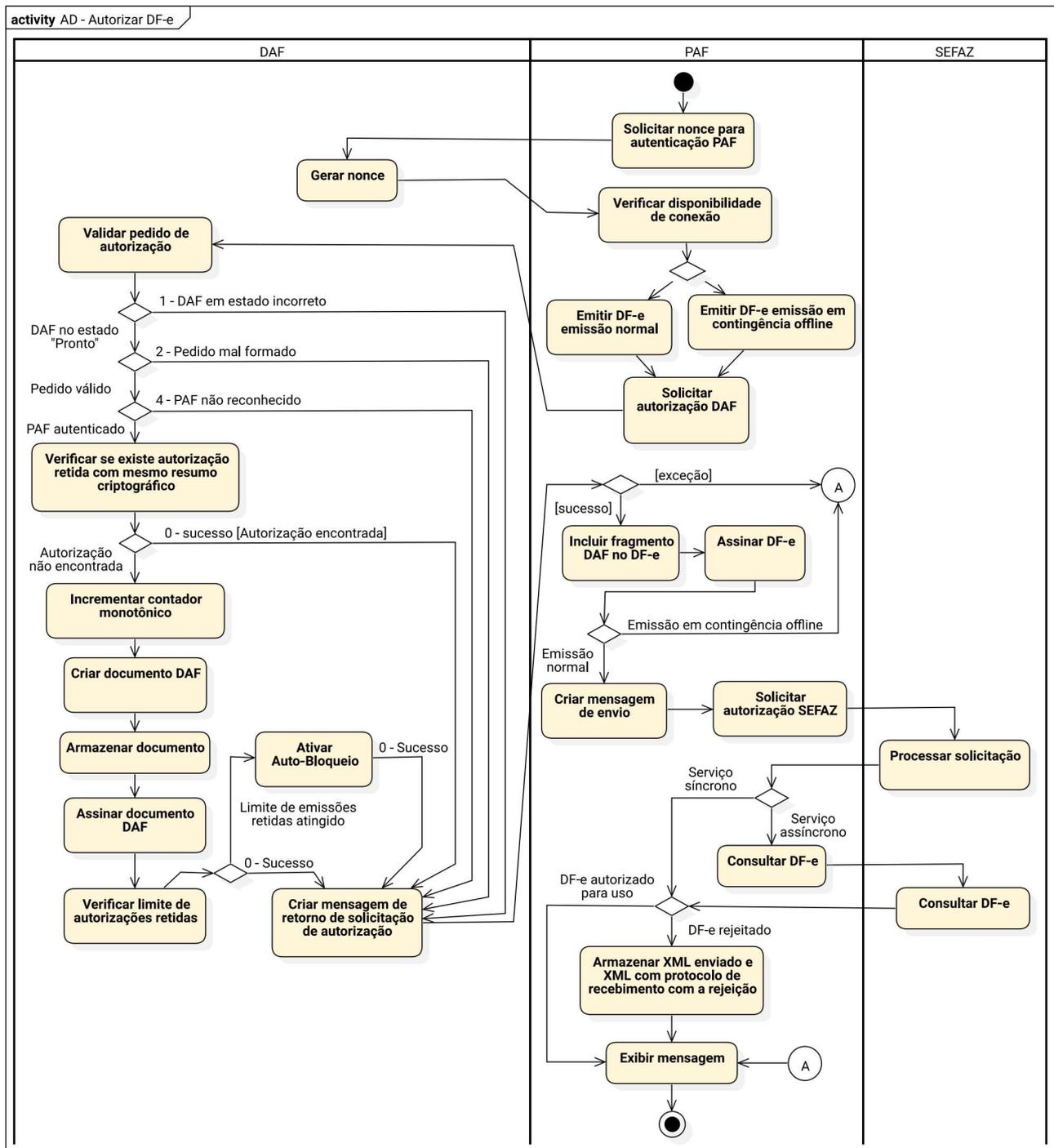
O documento XML com conjunto de informações essenciais do DF-e NÃO DEVE conter caracteres de nova linha e espaços em branco, cujo único objetivo seja para facilitar a legibilidade e que sejam insignificantes para a informação que está sendo carregada.

5.2.2 Representação da autorização gerada pelo DAF

Uma autorização gerada pelo DAF DEVE ser representada como um *token JSON Web Token (JWT)* ([JONES; BRADLEY; SAKIMURA, 2015](#)) (veja [Subseção 6.1.1](#)). O *token* JWT DEVE ter sua

diagrama de atividade UML, especificando as exceções possíveis no processo de autorização de um DF-e utilizando o DAF.

Figura 5.4: Diagrama de atividade do processo de autorização de um DF-e

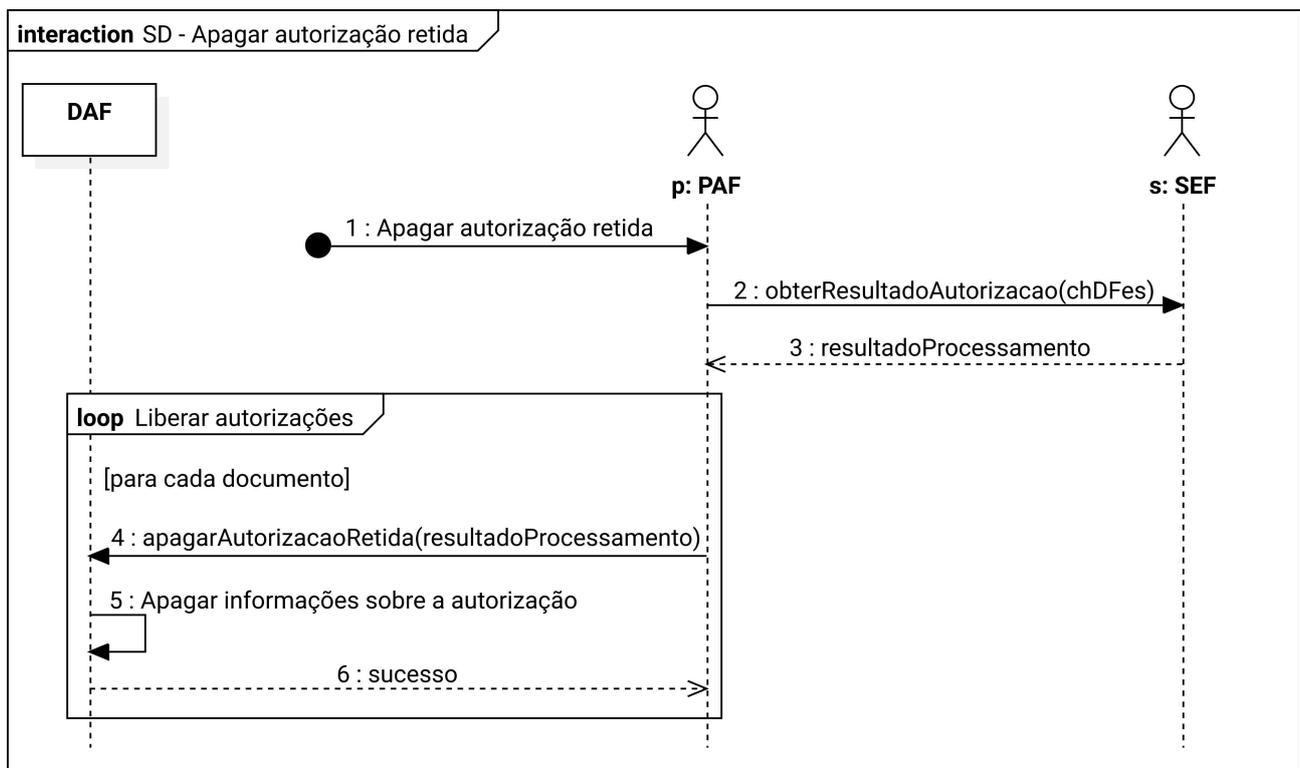


5.3 Apagar autorizações retidas no DAF

Ao autorizar um documento, o DAF mantém os dados sobre a autorização (veja [Seção 5.2](#)) em sua MT até que o PAF lhe encaminhe um documento, emitido pela SEF, que permita a exclusão dessa autorização. Sendo assim, após realizar o envio do DF-e à SEFAZ autorizadora e obter a autorização de uso, o PAF do contribuinte DEVE, posteriormente, solicitar o resultado sobre a autorização emitida pelo DAF junto à SEF e, por fim, encaminhar esse resultado ao DAF.

Na [Figura 5.5](#) é ilustrado um diagrama de sequência UML que, para facilitar o entendimento, contém somente o fluxo principal para apagar uma autorização retida na MT do DAF. Fluxos alternativos e de exceção para esse processo são apresentados no [Caso de Uso UC-4.2](#).

Figura 5.5: Diagrama de sequência do processo para apagar autorizações retidas



1. O processo pode ser iniciado pelo [contribuinte](#) ou por meio de uma rotina periódica do PAF para remoção de uma autorização retida na MT do DAF;
2. O PAF envia para a SEF uma lista contendo até 50 chaves de acesso dos DF-e cujas autorizações estão retidas no DAF (veja descrição do serviço na [Subseção 8.7.1](#));
3. A SEF retorna para o PAF um documento JSON com os resultados sobre a autorização para cada DF-e consultado. Para cada DF-e será retornado: sua chave de acesso, seu [idAut](#), o resultado da autorização e, caso a SEF considere que o DF-e pode ser removido do DAF, então também é enviada a saída de uma função HMAC que teve como chave a [chave SEF](#) e como mensagem o [idAut](#);
4. Para cada DF-e contido no documento recebido da SEF e que tenha recebido autorização para excluir a autorização retida, o PAF encaminha ao DAF seu [idAut](#) e a saída da função HMAC (veja descrição da mensagem na [Subsubseção 6.1.2.5](#));

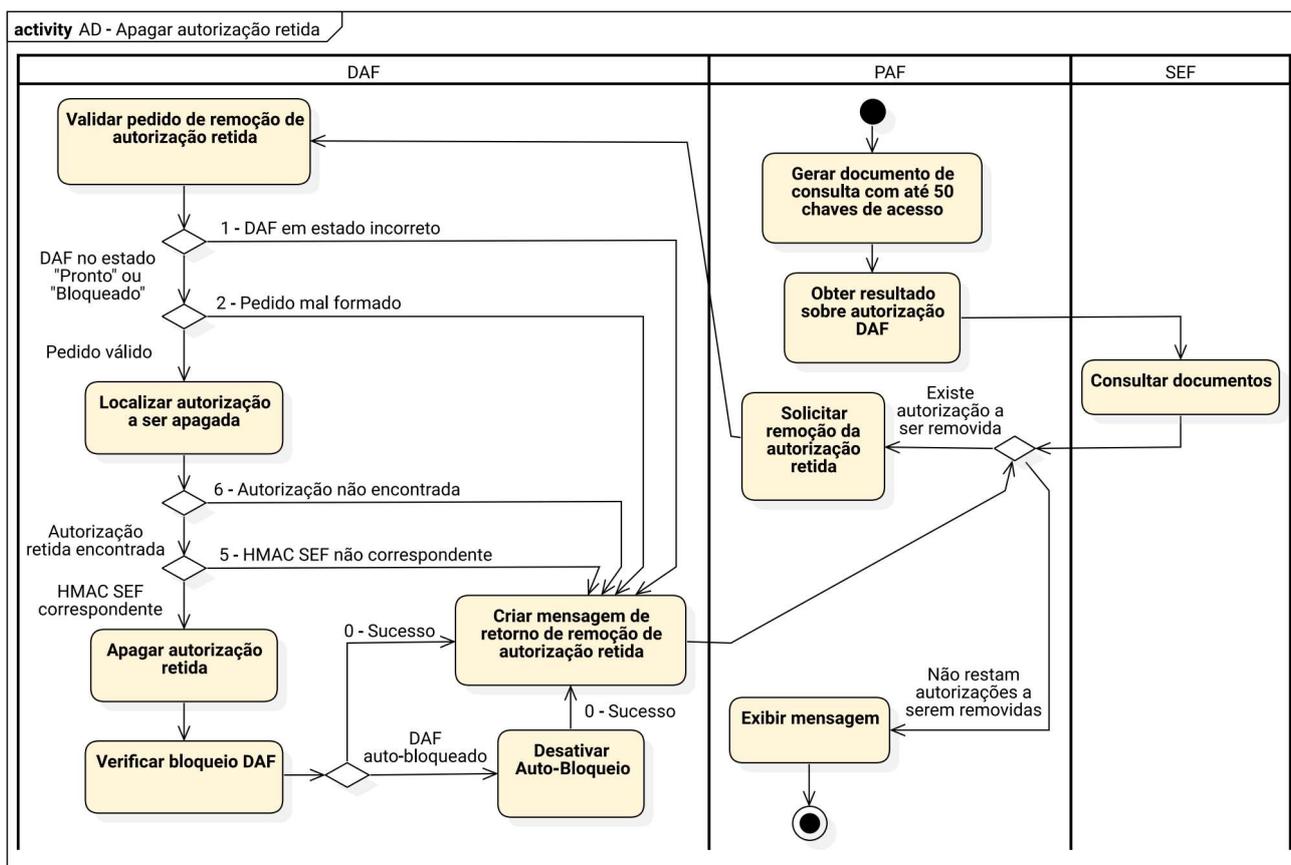
5. O DAF recebe o pedido e, em uma **transação atômica**:
 - 5.1. Verifica se seu estado atual é PRONTO ou BLOQUEADO (veja [Seção 2.2](#));
 - 5.2. Verifica se o pedido foi formado adequadamente;
 - 5.3. Verifica se o **idAut** está armazenado em sua MT;
 - 5.4. Gera um HMAC com as mesmas entradas que a SEF usou e, se houver correspondência, remove a autorização retida de sua MT de acordo com o **idAut** recebido.
6. O DAF retorna a mensagem de sucesso ao PAF.

Exemplos de mensagens para os comandos do DAF e serviços providos pela SEF envolvidos neste processo são apresentados na [Seção B.4](#).

5.3.1 Exceções

Durante o processo, o PAF é responsável pela comunicação com o DAF e a SEF. Assim, caso um destes sistemas incorram em exceção, a mensagem será tratada pelo PAF. A [Figura 5.6](#) ilustra o diagrama de atividade UML, especificando as exceções possíveis no processo para apagar autorizações retidas na MT.

Figura 5.6: Diagrama de atividade do processo para apagar autorizações retidas

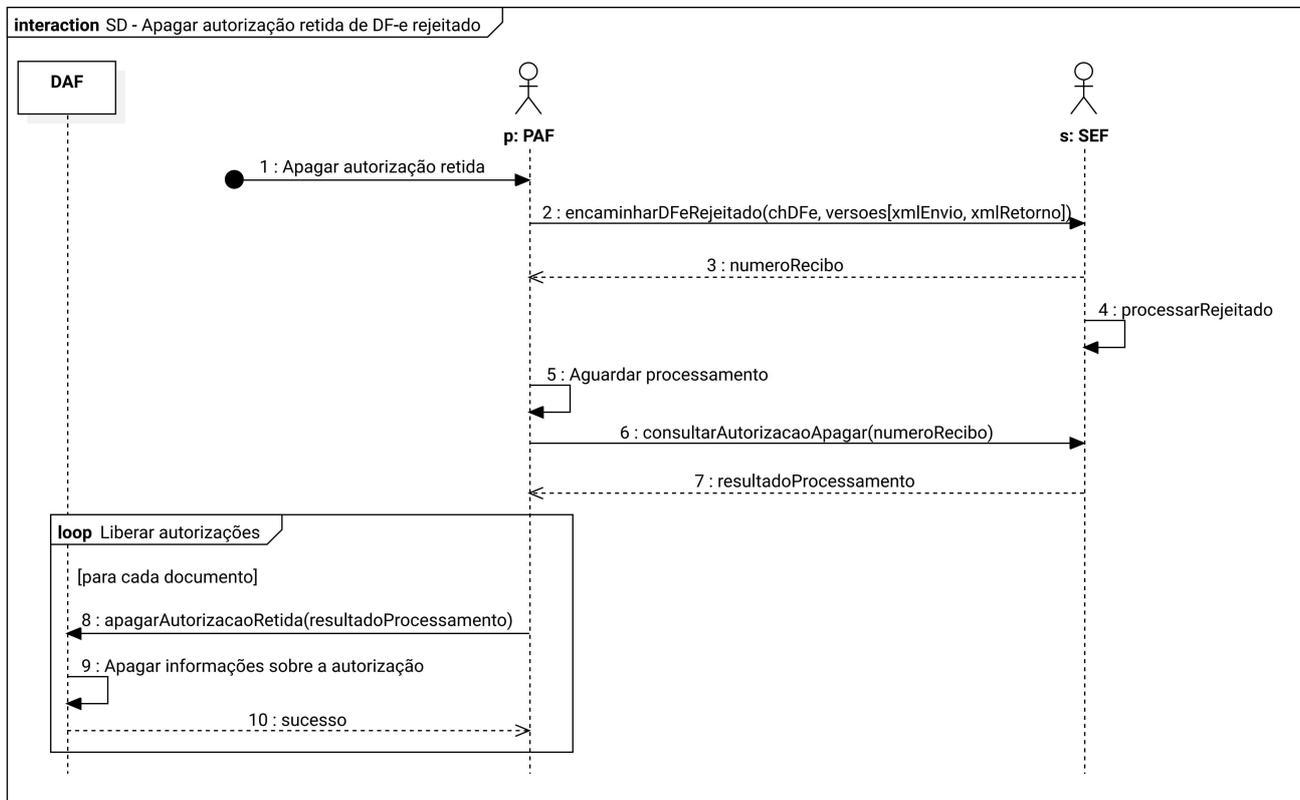


5.4 Apagar autorizações retidas no DAF sobre DF-e com rejeição

Para apagar as autorizações retidas de DF-e rejeitados pela SEFAZ autorizadora, deve-se fazer uso do serviço descrito em [Subseção 7.6.10](#). Na [Figura 5.7](#) é ilustrado um diagrama de sequência UML

que, para facilitar o entendimento, contém somente o fluxo principal para apagar uma autorização retida na MT do DAF que foram emitidas sobre documentos que resultaram em rejeição. Fluxos alternativos e de exceção para esse processo são apresentados no [Caso de Uso UC-4.2](#) e na [Seção 5.3](#).

Figura 5.7: Diagrama de sequência do processo para apagar autorizações retidas, de documentos com rejeições



1. O processo pode ser iniciado pelo [contribuinte](#) ou por meio de uma rotina periódica do PAF para remoção de uma autorização retida na MT do DAF;
2. O PAF encaminha para a SEF a chave de acesso do [DF-e](#) e até 20 versões rejeitadas pela SEFAZ, ordenadas cronologicamente, o que inclui o XML do [DF-e](#) encaminhado à SEFAZ e o respectivo protocolo de recebimento do [DF-e](#) que contém o motivo da rejeição (veja descrição do serviço na [Subseção 8.8.1](#));
3. A SEF registra a solicitação e retorna um número de recibo o qual deverá ser usado pelo PAF em uma consulta posterior, uma vez que este é um processo assíncrono;
4. A SEF inicia o processo de validação das informações recebidas;
5. O PAF deve aguardar um tempo mínimo antes que possa questionar a SEF sobre o resultado do processamento. A especificação do tempo mínimo está fora do escopo deste documento e tal informação deverá ser consultada na especificação de requisitos do PAF;
6. O PAF solicita o resultado do processamento, informando o número de recibo que foi obtido no passo 3 (veja descrição do serviço na [Subseção 8.8.3](#));
7. A SEF retorna para o PAF um documento JSON com os resultados sobre a autorização DAF para cada uma das versões rejeitadas do [DF-e](#) consultado. Para cada versão rejeitada será

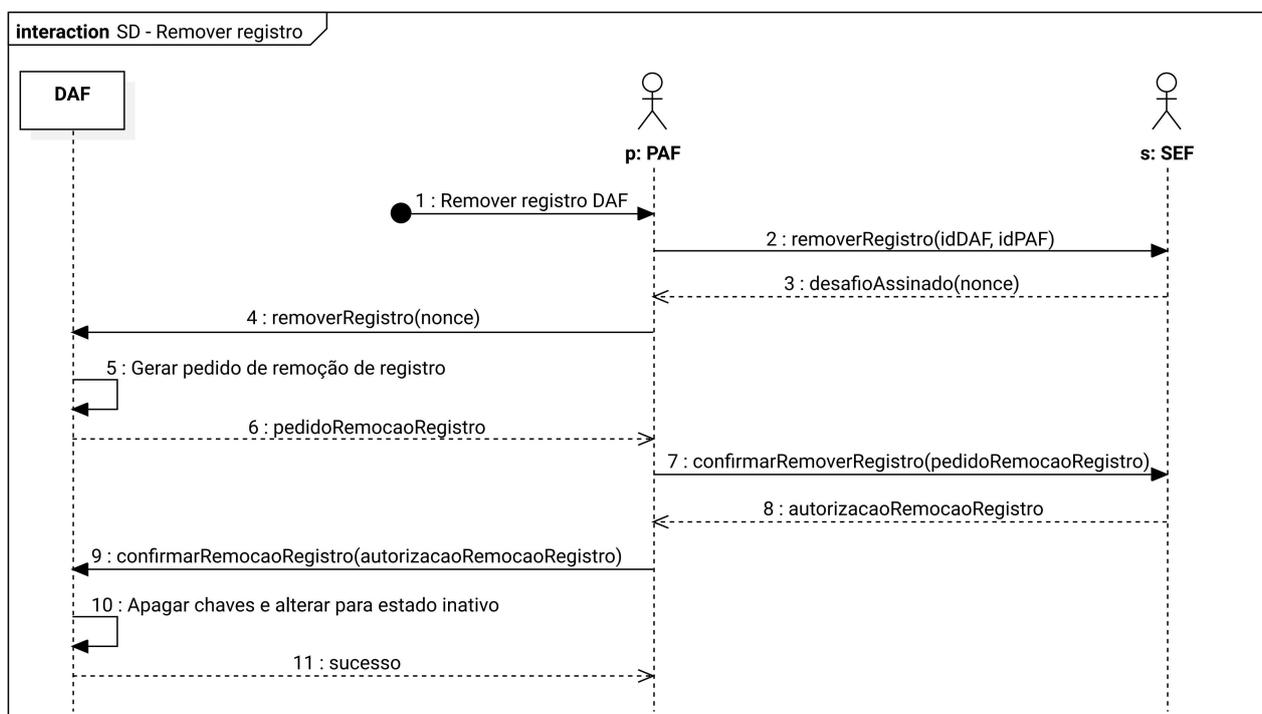
retornado: o **idAut**, o resultado da autorização e, caso a SEF considere que o DF-e pode ser removido do DAF, então também é enviada a saída de uma função **HMAC** que teve como chave a **chave SEF** e como mensagem o **idAut**;

8. Para cada versão rejeitada do DF-e contida no documento recebido da SEF e que recebeu autorização para excluir a autorização retida, o PAF encaminha ao DAF seu **idAut** e a saída da função HMAC (veja descrição da mensagem na [Subsubseção 6.1.2.5](#));
9. O DAF recebe o pedido e, em uma **transação atômica**:
 - 9.1. Verifica se seu estado atual é PRONTO ou BLOQUEADO (veja [Seção 2.2](#));
 - 9.2. Verifica se o pedido foi formado adequadamente;
 - 9.3. Verifica se o **idAut** está armazenado em sua MT;
 - 9.4. Gera um HMAC com as mesmas entradas que a SEF usou e, se houver correspondência, remove a autorização retida de sua MT de acordo com o **idAut** recebido.
10. O DAF retorna a mensagem de sucesso ao PAF.

5.5 Remover registro do DAF junto à SEF

Na [Figura 5.8](#) é ilustrado um diagrama de sequência UML que, para facilitar o entendimento, contém somente o fluxo principal para remover o registro do DAF junto à SEF. Fluxos alternativos e de exceção para esse processo são apresentados nos Casos de Uso [UC-4.11](#) e [UC-4.2](#).

Figura 5.8: Diagrama de sequência do processo para remover o registro do DAF junto à SEF



1. O processo é iniciado pelo **contribuinte**, o qual invoca a rotina específica do PAF para remover o registro do DAF junto à SEF;

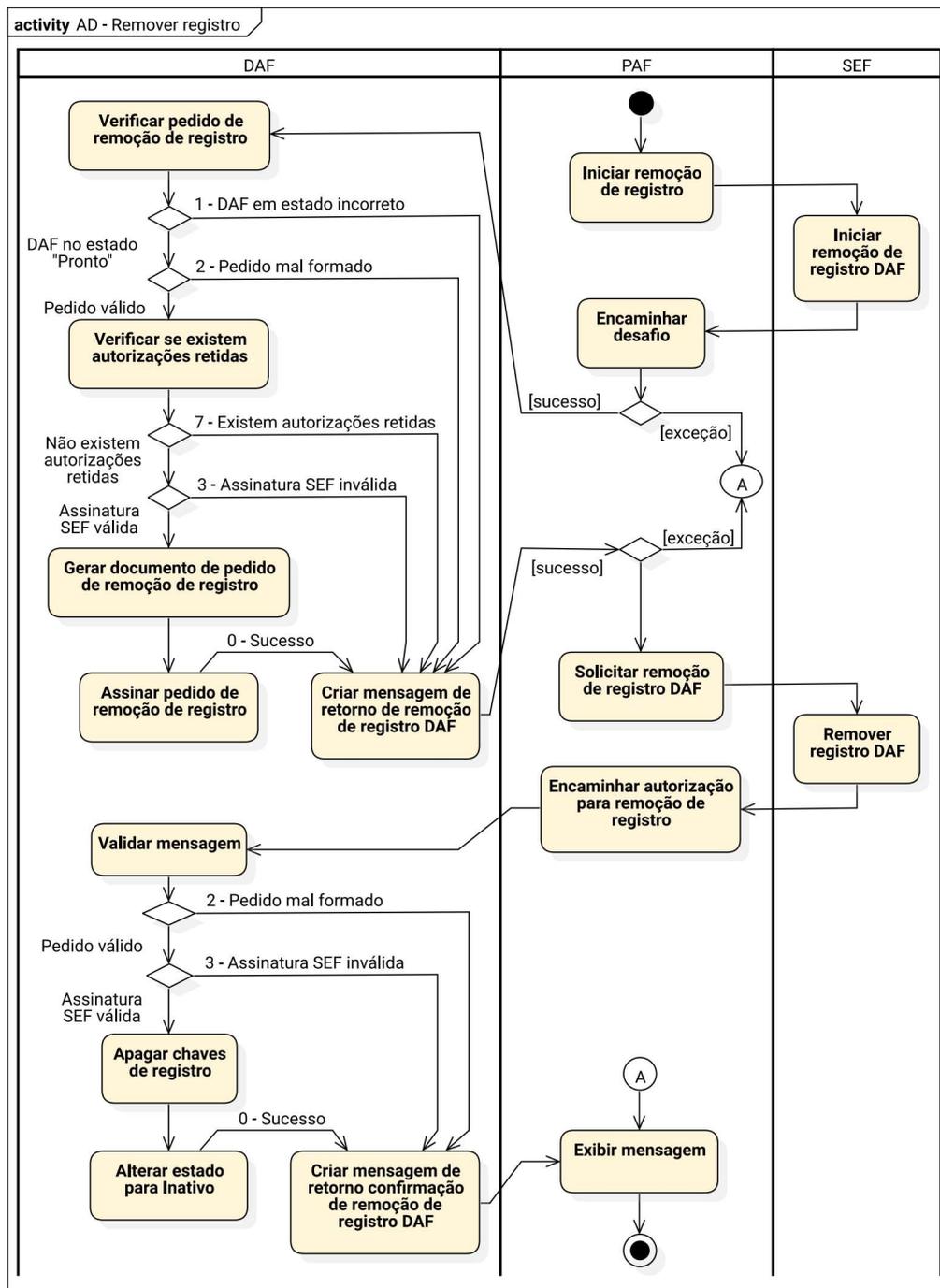
2. O PAF envia para SEF um pedido para iniciar o processo de remoção de registro do DAF. No pedido DEVE constar o [IdDAF](#) e o [IdPAF](#) (veja descrição do serviço na [Subseção 8.6.1](#));
3. A SEF processa o pedido de remoção de registro, gera um *nonce*, armazena-o e prepara um documento estruturado contendo o *nonce* gerado. Esse documento é então assinado com a [chave privada](#) correspondente à [chave pública](#) contida no [certificado digital da SEF](#) e retornado ao PAF;
4. O PAF encaminha ao DAF o documento recebido da SEF (veja descrição da mensagem na [Subsubseção 6.1.2.6](#));
5. O DAF recebe o pedido e, em uma [transação atômica](#):
 - 5.1. Verifica se seu estado atual é PRONTO (veja [Seção 2.2](#));
 - 5.2. Verifica se o pedido foi formado adequadamente;
 - 5.3. Verifica se existem autorizações retidas em sua MT;
 - 5.4. Verifica se a assinatura da SEF sobre a mensagem é válida;
 - 5.5. Gera um documento de solicitação de remoção de registro o qual contém seu [IdDAF](#), o atual valor de seu [contador monotônico](#) e o *nonce* recebido pela SEF. Esse documento é então assinado com a [chave privada do DAF](#).
6. O DAF retorna para o PAF o documento gerado no passo anterior;
7. O PAF encaminha à SEF o documento gerado pelo DAF (veja descrição do serviço na [Subseção 8.6.2](#));
8. A SEF recebe o pedido de remoção de registro e:
 - 8.1. Verifica a correspondência do *nonce* e se a assinatura do documento gerada pela chave privada do DAF é válida;
 - 8.2. Remove o registro do DAF e gera um documento estruturado contendo a cadeia de caracteres REMOVE. Esse documento é então assinado com a [chave privada](#) correspondente à [chave pública](#) contida no [certificado digital da SEF](#) e retornado ao PAF.
9. O PAF encaminha ao DAF o documento recebido da SEF (veja descrição da mensagem na [Subsubseção 6.1.2.7](#));
10. O DAF recebe o pedido e, em uma [transação atômica](#):
 - 10.1. Verifica se o pedido foi formado adequadamente e se o documento encaminhado contém a cadeia de caracteres REMOVE;
 - 10.2. Verifica se a assinatura da SEF sobre a mensagem é válida;
 - 10.3. Apaga de sua memória segura a [chave privada do DAF](#), a [chave SEF](#) e a [chave PAF](#), e altera seu estado para INATIVO.
11. O DAF retorna a mensagem de sucesso ao PAF.

Exemplos de mensagens para os comandos do DAF e serviços providos pela SEF envolvidos neste processo são apresentados na [Seção B.2](#).

5.5.1 Exceções

Durante o processo, o PAF é responsável pela comunicação com o DAF e a SEF. Assim, caso um destes sistemas incorram em exceção, a mensagem será tratada pelo PAF. A Figura 5.9 ilustra o diagrama de atividade UML, especificando as exceções possíveis no processo para remover o registro DAF.

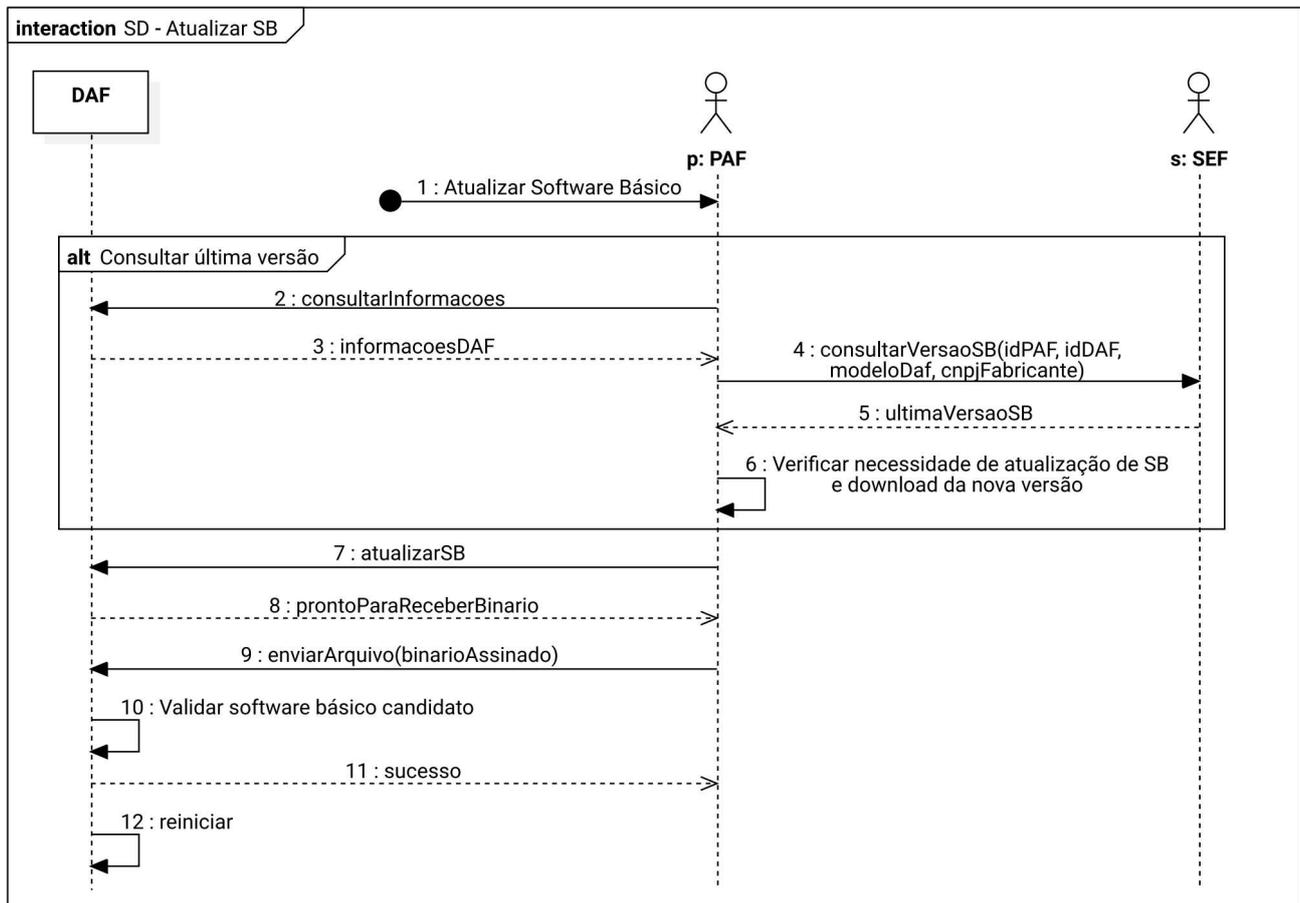
Figura 5.9: Diagrama de atividade do processo para remover o registro do DAF junto à SEF



5.6 Atualizar Software Básico

Na [Figura 5.10](#) é ilustrado um diagrama de sequência UML que, para facilitar o entendimento, contém somente o fluxo principal para atualizar o SB do DAF. Fluxos alternativos e de exceção para esse processo são apresentados no Casos de Uso [UC-4.5](#) e [UC-4.7](#).

Figura 5.10: Diagrama de sequência do processo para atualizar o SB do DAF



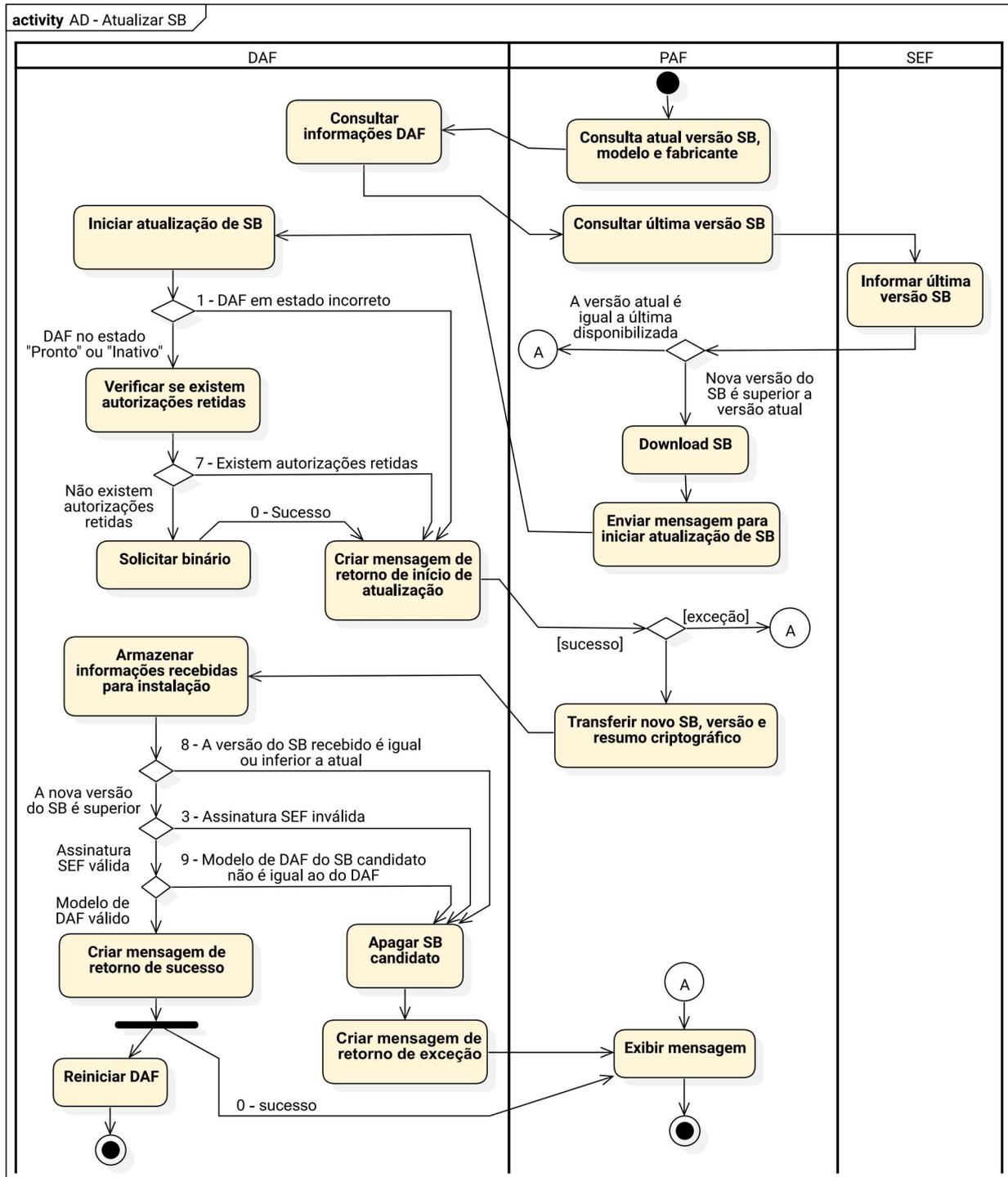
1. O processo pode ser iniciado pelo [contribuinte](#) ou por meio de uma rotina periódica do PAF para atualizar o SB do DAF;
2. O PAF solicita ao DAF suas informações (veja descrição da mensagem na [Subsubseção 6.1.2.8](#));
3. O DAF retorna suas informações;
4. O PAF solicita à SEF informações sobre a última versão de SB disponibilizada pelo fabricante do DAF, neste pedido devem constar o [IdPAF](#), o [IdDAF](#), CNPJ do fabricante do DAF e o nome do modelo do DAF (veja descrição do serviço na [Subseção 8.11.1](#));
5. A SEF envia ao PAF um documento estruturado contendo a versão do último SB para o modelo de DAF recebido, bem como a [URL](#) onde o binário do SB pode ser baixado, a data de publicação do novo SB e o [resumo criptográfico](#) sobre o binário do novo SB;
6. O PAF verifica que a versão de SB instalada no DAF é inferior a versão de SB informada pela SEF e baixa o binário do SB a partir da URL informada pela SEF;
7. O PAF informa ao DAF que iniciará o processo de atualização de SB (veja descrição da mensagem na [Subsubseção 6.1.2.9](#));

8. O DAF recebe o pedido e:
 - 8.1. Verifica se está no estado PRONTO ou INATIVO;
 - 8.2. Verifica se possui autorizações retidas em sua MT;
9. O DAF responde ao PAF que está pronto para a atualização de SB;
10. O PAF transfere para o DAF o binário do SB (veja descrição do comando na [Subseção 6.2.4](#));
11. O DAF armazena o binário do SB candidato na sua partição de atualização e, em uma [transação atômica](#):
 - 11.1. Verifica se a versão do SB recebido é superior à versão instalada;
 - 11.2. Verifica, por meio da assinatura gerada pela SEF, a integridade e autenticidade do binário recebido;
 - 11.3. Por meio da assinatura gerada pelo fabricante, usando a [chave de ateste](#) do DAF, verifica se o SB recebido é o correto para o modelo de DAF em questão;
 - 11.4. O DAF informa ao PAF que o SB foi recebido com sucesso;
 - 11.5. O DAF é reiniciado automaticamente.

5.6.1 Exceções

Durante o processo, o PAF é responsável pela comunicação com o DAF e a SEF. Assim, caso um destes sistemas incorram em exceção, a mensagem será tratada pelo PAF. A [Figura 5.11](#) ilustra o diagrama de atividade UML, especificando as exceções possíveis no processo para atualizar o SB do o DAF.

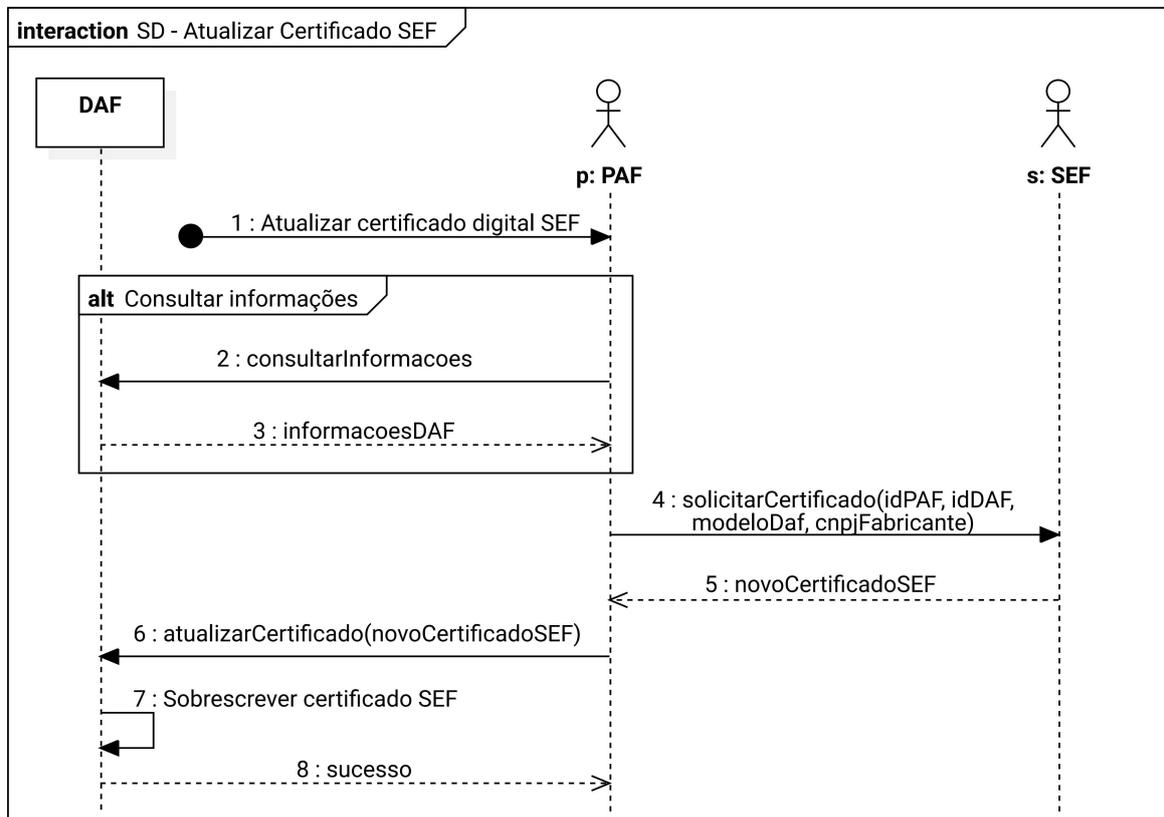
Figura 5.11: Diagrama de atividade do processo para atualizar o SB do DAF



5.7 Atualizar certificado digital SEF

Na [Figura 5.12](#) é ilustrado um diagrama de sequência UML que, para facilitar o entendimento, contém somente o fluxo principal para atualizar o certificado digital da SEF armazenado no DAF. Fluxos alternativos e de exceção para esse processo são apresentados no [Caso de Uso UC-4.4](#).

Figura 5.12: Diagrama de sequência do processo para atualizar o certificado digital SEF no DAF



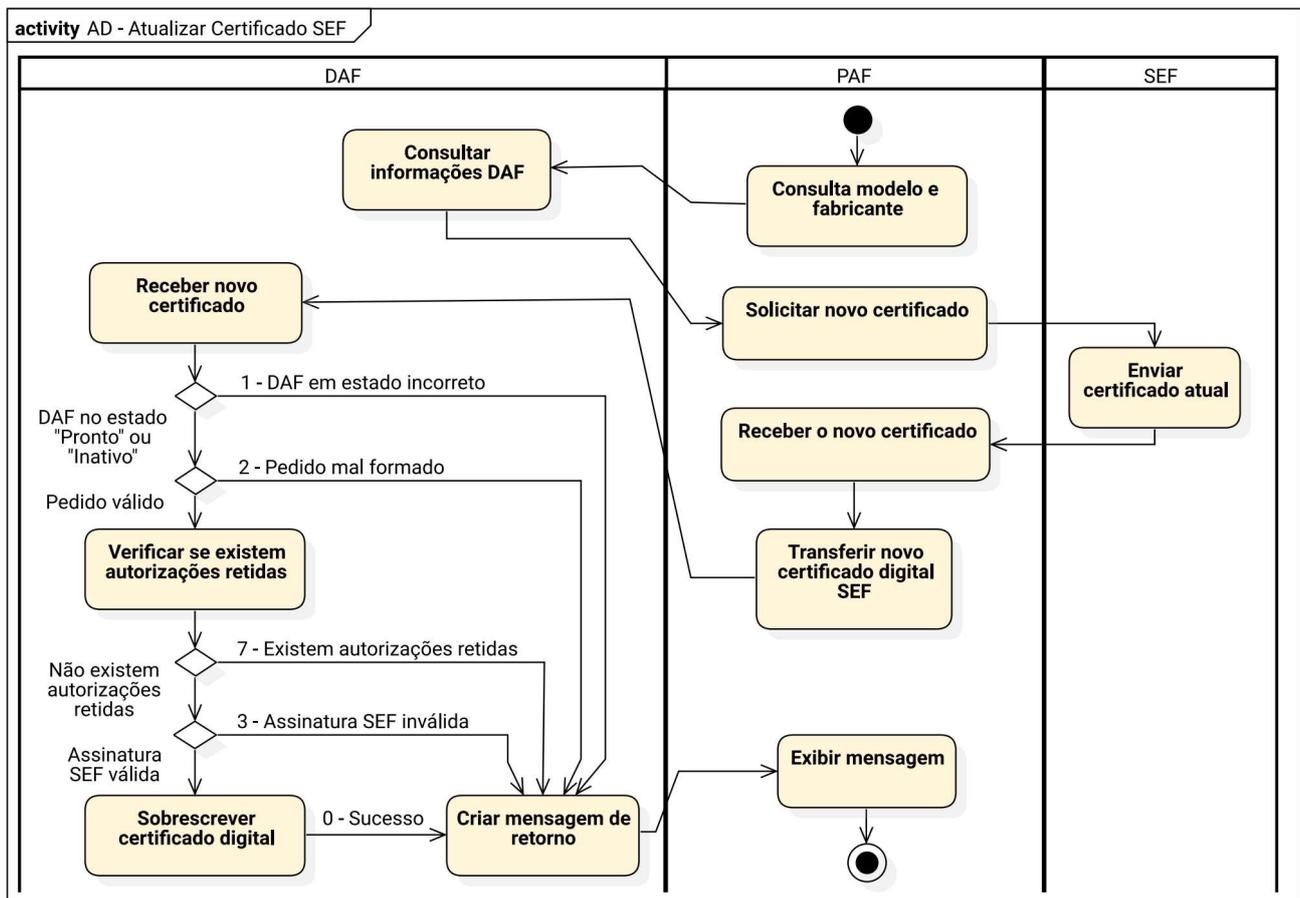
1. O processo é iniciado pelo **contribuinte**, o qual invoca a rotina específica do PAF para atualizar o certificado digital SEF armazenado no DAF;
2. O PAF solicita ao DAF suas informações (veja descrição da mensagem na [Subsubseção 6.1.2.8](#));
3. O DAF retorna suas informações;
4. O PAF solicita à SEF o atual certificado digital válido para o DAF que opera. No pedido são enviados o **IdPAF**, o **IdDAF**, CNPJ do fabricante do DAF e o nome do modelo do DAF (veja descrição do serviço na [Subseção 8.12.1](#));
5. A SEF retorna um arquivo contendo o certificado digital codificado no formato textual **PEM** ([JOSEFSSON; LEONARD, 2015](#));
6. O PAF transfere para o DAF o certificado digital recebido da SEF (veja descrição da mensagem na [Subsubseção 6.1.2.10](#));
7. O DAF recebe o novo certificado e, em uma **transação atômica**:
 - 7.1. Verifica se está no estado PRONTO ou INATIVO;
 - 7.2. Verifica se o pedido foi formado adequadamente;

- 7.3. Verifica se possui autorizações retidas em sua MT;
 - 7.4. Verifica se o novo certificado foi assinado com a **chave privada** correspondente à **chave pública** presente no atual **certificado digital da SEF** que o DAF possui;
 - 7.5. Sobrescreve **certificado digital da SEF**.
8. O DAF retorna uma mensagem de sucesso ao PAF, que por sua vez informa ao usuário;

5.7.1 Exceções

Durante o processo, o PAF é responsável pela comunicação com o DAF e a SEF. Assim, caso um destes sistemas incorram em exceção, a mensagem será tratada pelo PAF. A **Figura 5.13** ilustra o diagrama de atividade UML, especificando as exceções possíveis no processo para atualizar o certificado SEF armazenado no DAF.

Figura 5.13: Diagrama de atividade do processo para atualizar o certificado digital SEF no DAF

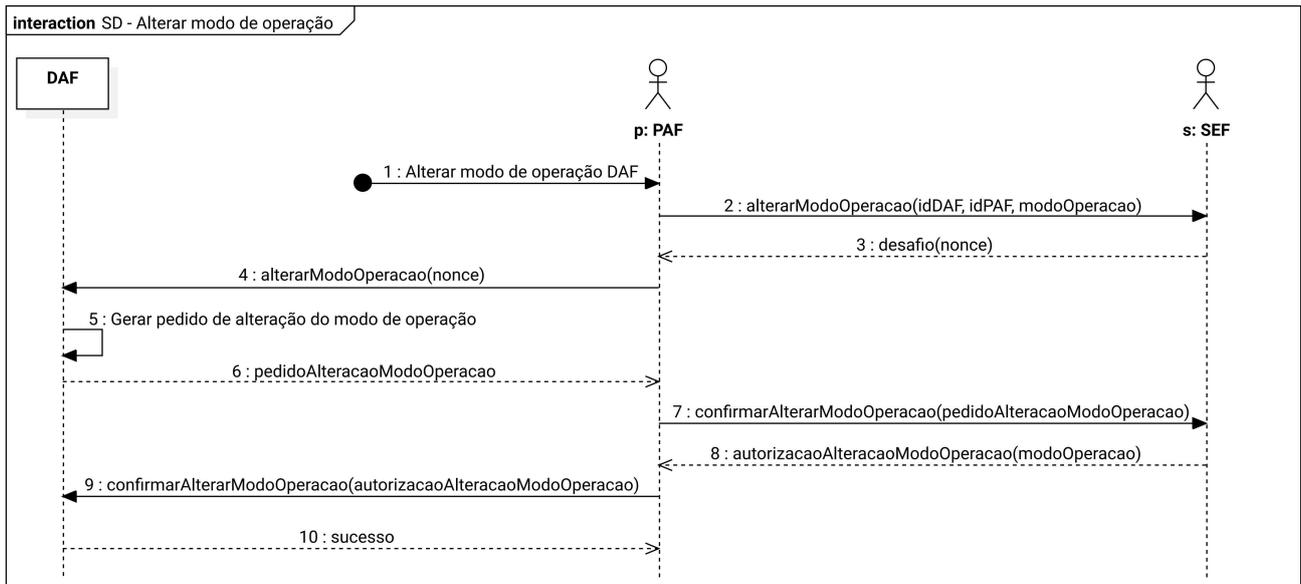


5.8 Alterar modo de operação do DAF

Na **Figura 5.14** é ilustrado um diagrama de sequência UML que, para facilitar o entendimento, contém somente o fluxo principal para alterar o **modo de operação do DAF**. Fluxos alternativos e de exceção para esse processo são apresentados no Caso de Uso **UC-4.1**.

1. O processo é iniciado pelo **contribuinte**, o qual invoca a rotina específica do PAF para alterar o **modo de operação do DAF**;

Figura 5.14: Diagrama de seqüência do processo para alterar o modo de operação do DAF



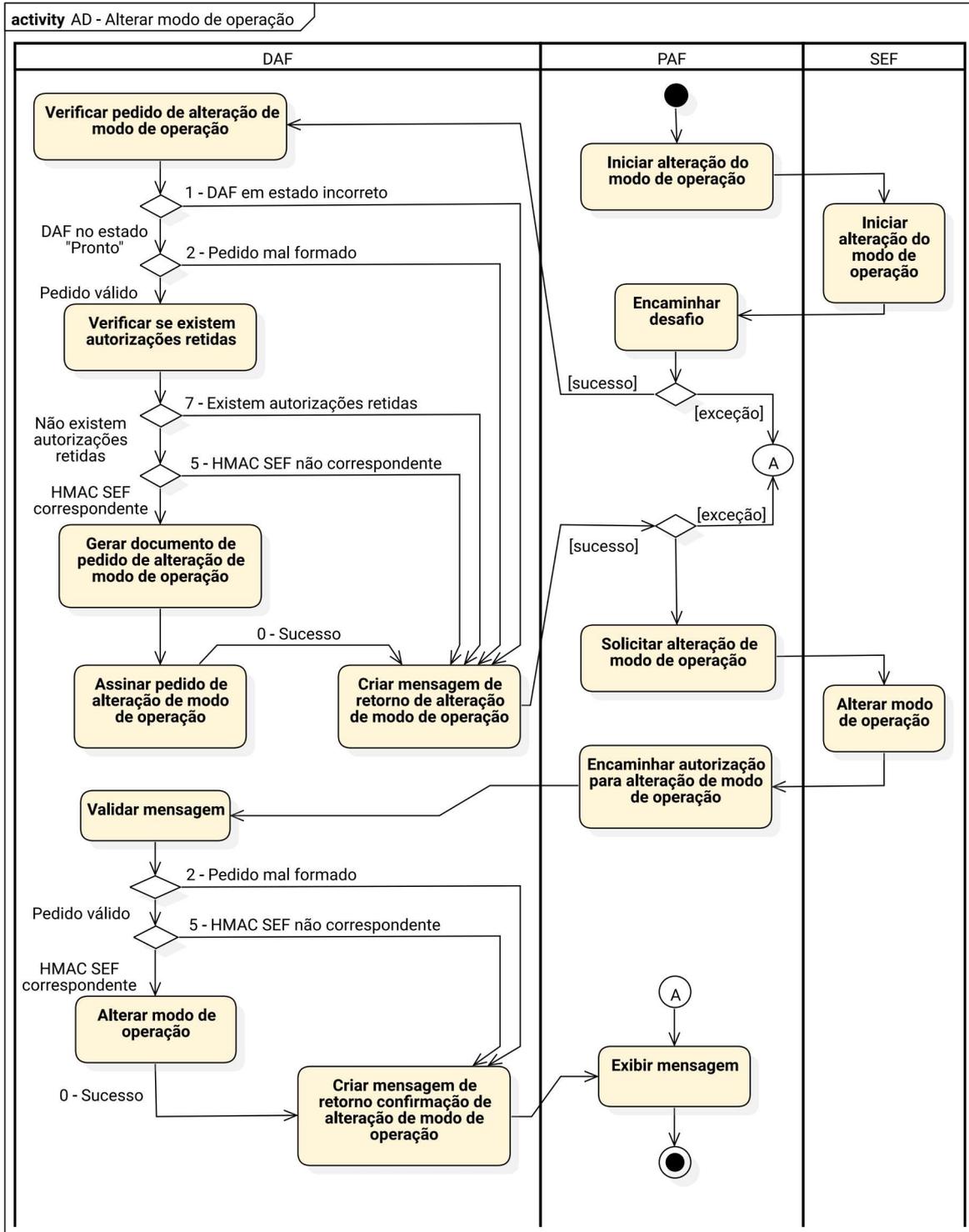
2. O PAF envia para SEF um pedido para iniciar o processo de alteração do modo de operação do DAF. No pedido DEVE constar o **IdDAF**, o **IdPAF** e o novo valor para o **modo de operação do DAF** (veja descrição do serviço na [Subseção 8.10.1](#));
3. A SEF verifica se o valor informado para o **modo de operação do DAF** é um valor permitido, gera um *nonce*, armazena-o e retorna para o PAF um documento estruturado contendo o *nonce* gerado, cuja integridade e autenticidade é garantida por meio de uma função HMAC que teve como chave a **chave SEF** e como mensagem o documento que contém o *nonce*;
4. O PAF encaminha ao DAF o documento recebido da SEF (veja descrição da mensagem na [Subsubseção 6.1.2.12](#));
5. O DAF recebe o pedido e:
 - 5.1. Verifica se seu estado atual é PRONTO (veja [Seção 2.2](#));
 - 5.2. Verifica se o pedido foi formado adequadamente;
 - 5.3. Verifica se existem autorizações retidas em sua MT;
 - 5.4. Verifica a integridade e autenticidade da mensagem recebida por meio de uma função HMAC que teve como chave a **chave SEF** e como mensagem o documento que contém o *nonce* gerado pela SEF;
 - 5.5. Gera um documento de solicitação de alteração do modo de operação do DAF, o qual contém seu **IdDAF**, o atual valor de seu **contador monotônico** e o *nonce* recebido pela SEF.
6. O DAF retorna para o PAF um documento estruturado, cuja integridade e autenticidade é garantida por meio de uma função HMAC que teve como chave a **chave SEF**, contendo o documento gerado no passo anterior;
7. O PAF encaminha à SEF o documento gerado pelo DAF (veja descrição do serviço na [Subseção 8.10.2](#));
8. A SEF recebe o pedido de alteração do modo de operação do DAF e:

- 8.1. Verifica a correspondência do *nonce*, a integridade e autenticidade do documento recebido por meio de uma função HMAC que teve como chave a *chave SEF* e como mensagem o documento estruturado gerado pelo DAF;
 - 8.2. Altera o *modo de operação do DAF* junto ao seu registro e gera um documento contendo o novo valor para o *modo de operação do DAF*;
 - 8.3. Retorna para o PAF um documento estruturado, cuja integridade e autenticidade é garantida por meio de uma função HMAC que teve como chave a *chave SEF*, contendo o documento gerado no passo anterior.
9. O PAF encaminha ao DAF o documento recebido da SEF (veja descrição da mensagem na [Subsubseção 6.1.2.13](#));
10. O DAF recebe o pedido e:
- 10.1. Verifica se o pedido foi formado adequadamente e se e se o documento encaminhado contém o novo modo de operação do DAF
 - 10.2. Verifica a integridade e autenticidade da mensagem recebida por meio de uma função HMAC que teve como chave a *chave SEF* e como mensagem o documento estruturado que contém o novo valor do *modo de operação do DAF* encaminhado pela SEF;
 - 10.3. Altera o valor de seu modo de operação do DAF.
11. O DAF retorna a mensagem de sucesso ao PAF.

5.8.1 Exceções

Durante o processo, o PAF é responsável pela comunicação com o DAF e a SEF. Assim, caso um destes sistemas incorram em exceção, a mensagem será tratada pelo PAF. A [Figura 5.15](#) ilustra o diagrama de atividade UML, especificando as exceções possíveis no processo para alterar o *modo de operação do DAF*.

Figura 5.15: Diagrama de atividade do processo para alterar modo de operação do DAF



6 Protocolo de comunicação

O DAF é um dispositivo passivo que só reage mediante a um estímulo do PAF. Dessa forma, o protocolo de comunicação do DAF está fundamentado sobre o modelo de pedido e resposta, ou seja, depois que um pedido foi solicitado pelo PAF, esse pedido deve ser totalmente concluído pelo DAF ou abortado pelo PAF antes que um segundo pedido possa ser feito.

De forma a estruturar a implementação, nas próximas seções, a especificação do protocolo do DAF está dividida em dois níveis: i) API DAF – de mais alto nível, imutável e onde se define os pedidos e respostas para implementação dos processos operacionais apresentados no [Capítulo 4](#) e no [Capítulo 5](#); ii) Protocolo de transporte – mecanismos definidos a partir das características da interface de comunicação adotada pelo DAF, sendo atualmente apenas a interface USB.

6.1 API DAF

O conjunto de pedido e resposta trocado entre o DAF e o PAF para a implementação dos casos de uso e processos operacionais (veja [Capítulo 4](#) e [Capítulo 5](#)) pode ser visto como uma *Application Programming Interface (API)*, sendo o PAF o principal cliente dessa API. As mensagens trocadas entre o DAF e o PAF são síncronas e características como entrega confiável e ordenação dos pedidos e respostas devem ser tratadas diretamente pela tecnologia de transporte subjacente. Sendo assim, todo pedido recebido pelo DAF terá uma resposta assim que o DAF terminar seu processamento.

6.1.1 Representação dos pedidos e respostas da API DAF

Para que o DAF possa atender seu propósito, os pedidos e respostas DEVEM ser trocados de acordo com os casos de uso apresentados na [Seção 4.1](#) e os processos apresentados no [Capítulo 5](#). Os pedidos e respostas da API DAF (veja [Subseção 6.1.2](#)) devem ser representados de acordo com as seguintes regras:

1. Os pedidos e respostas DEVEM ser representados como documentos textuais *JavaScript Object Notation (JSON)* (BRAY, 2017) e os valores no documento JSON deverão ser representados de acordo com seu tipo e característica;
 - 1.1. O documento JSON DEVE ser gerado de forma minimizada, sem espaços em branco ou quebras de linha entre as chaves e os valores do documento.
2. O código do pedido ou o código da resposta (veja [Tabela 6.1](#) e [Tabela 6.2](#)) DEVE aparecer como o primeiro par de chave e valor no documento JSON. Para o pedido DEVE ser usada a chave `msg` e para a resposta DEVE ser usada a chave `res`;

3. Em pedidos ou respostas, cujo conteúdo não seja assinado digitalmente, os nomes dos parâmetros e seus valores DEVEM ser representados como pares chave e valor e DEVEM estar na mesma ordem dentro do documento JSON conforme apresentado na [Subseção 6.1.2](#) (veja exemplo de representação de pedido e resposta sem assinatura digital na [Seção A.1](#) e na [Seção A.2](#));
4. Em pedidos ou respostas, cujo conteúdo seja assinado digitalmente:
 - 4.1. O documento JSON DEVE conter apenas a chave `msg` para o pedido e `res` para respostas, além da chave `jwt` que DEVE conter como valor um *token JWT* (JONES; BRADLEY; SAKIMURA, 2015) (veja exemplo de representação de pedido e resposta assinados na [Seção A.3](#) e na [Seção A.4](#));
 - 4.2. No cabeçalho (*header*) do *token JWT* DEVEM constar somente as chaves `typ` e `alg`, com seus respectivos valores, com informações sobre o algoritmo criptográfico utilizado para gerar a assinatura do *token*:
 - 4.2.1. Para pedidos ou respostas que precisarem indicar explicitamente a *chave pública*, par da *chave privada* que foi usada para assinar o *token*, essa deverá ser representada dentro do cabeçalho do `jwt`, de acordo com as especificações *JSON Web Key (JWK)* (JONES, 2015b) e *JSON Web Algorithms (JWA)* (JONES, 2018);
 - 4.2.2. O documento JSON do cabeçalho (*header*) do *token JWT* DEVE ser gerado de forma minimizada, sem espaços em branco ou quebras de linha entre as chaves e os valores do documento.
 - 4.3. No conteúdo (*payload*) do *token JWT* os nomes dos parâmetros e seus valores DEVEM ser representados como pares chave e valor e DEVEM estar na mesma ordem dentro do documento JSON conforme apresentado na [Subseção 6.1.2](#);
 - 4.3.1. O documento JSON do conteúdo (*payload*) do *token JWT* DEVE ser gerado de forma minimizada, sem espaços em branco ou quebras de linha entre as chaves e os valores do documento.
5. Documentos XML, quando representados como valores nos documentos JSON DEVEM sofrer as seguintes transformações:
 - 5.1. Caracteres de nova linha DEVEM ser removidos;
 - 5.2. Espaços em branco usados somente para facilitar a legibilidade e que sejam insignificantes para a informação que está sendo carregada DEVEM ser removidos;
 - 5.3. O documento XML resultante DEVE ser convertido para Base64URL (JOSEFSSON, 2006);
6. Todo *nonce* em documentos JSON DEVE ser representado em Base64URL;
7. Todo *resumo criptográfico* em documentos JSON DEVE ser representado em Base64URL;
8. Toda informação transportada dentro de objetos JSON, representada em Base64URL, DEVE ser decodificada de Base64URL antes de ser processada pelo DAF ou pelo PAF, como por exemplo as informações utilizadas para geração de *HMAC*;

9. Os números inteiros, como o [contador monotônico](#), quando forem entradas de funções criptográficas, DEVEM ser representados na memória com a extremidade (*endianness*) *big-endian*.

6.1.2 Pedidos e respostas da API DAF

Na [Tabela 6.1](#) é apresentada a lista de pedidos da API DAF. Na tabela são apresentados o código de cada pedido, se possui parâmetros, o tipo de resposta que deverá gerar e o tempo máximo, em milissegundos, para o DAF processar o pedido recebido e encaminhar a resposta ao PAF. As respostas enviadas pelo DAF poderão ser de dois tipos: i) simples – quando contiver apenas o código da resposta; ii) completa – quando contiver o código da resposta e parâmetros adicionais.

1. O DAF DEVE implementar todos os pedidos apresentados na [Tabela 6.1](#) e as respostas apresentadas na [Tabela 6.2](#);
2. O DAF NÃO DEVE implementar nenhuma outro pedido ou resposta exclusiva do fabricante.

Tabela 6.1: Pedidos da API DAF

Nome do pedido	Código	Parâmetros	Tipo de resposta	Caso de uso	Tempo máximo (ms)
registrar	1	sim	completa	UC-4.10	800
confirmarRegistro	2	sim	simples	UC-4.10	200
solicitarAutenticacao	3	não	completa	UC-4.6	200
autorizarDFE	4	sim	completa	UC-4.6	200
apagarAutorizacaoRetida	5	sim	simples	UC-4.2	200
removerRegistro	6	sim	completa	UC-4.11	200
confirmarRemocaoRegistro	7	sim	simples	UC-4.11	200
consultarInformacoes	8	não	completa	UC-4.7	800
atualizarSB	9	não	simples	UC-4.5	200
atualizarCertificado	10	sim	simples	UC-4.4	200
descarregarRetido	11	sim	completa	UC-4.9	200
alterarModoOperacao	12	sim	completa	UC-4.1	200
confirmarAlterarModoOperacao	13	sim	simples	UC-4.1	200
cancelarProcesso	14	não	simples	-	200

Na [Listagem 6.1](#) é apresentado um exemplo de como uma resposta do tipo **simples**, gerada pelo DAF, DEVE ser representada. O valor associado a chave `res` DEVE ser um dos códigos de respostas apresentados na [Tabela 6.2](#).

Listagem 6.1: Documento JSON para resposta do tipo simples

```
1 {  
2   "res": 0  
3 }
```

Tabela 6.2: Códigos das respostas geradas pelo DAF

Nome da resposta	Valor	Descrição
<code>sucesso</code>	0	Sucesso no processamento do pedido
<code>estadoIncorreto</code>	1	DAF em estado incorreto
<code>pedidoMalFormado</code>	2	Pedido formado de forma inadequada
<code>assinaturaInvalida</code>	3	Assinatura SEF inválida
<code>pafDesconhecido</code>	4	PAF não reconhecido pelo DAF
<code>hmacNaoCorrespondente</code>	5	DAF não reconhece o HMAC recebido
<code>autorizacaoNaoEncontrada</code>	6	Autorização não encontrada na MT do DAF
<code>autorizacaoRetida</code>	7	DAF com autorizações retidas
<code>versaoSBInvalida</code>	8	Versão do SB inferior ou igual à versão existente
<code>modeloInvalido</code>	9	Modelo de DAF do SB candidato é diferente do modelo do DAF em questão

6.1.2.1 registrar

Esse pedido é enviado pelo PAF para iniciar o processo de registro do DAF junto à SEF (veja [Caso de Uso UC-4.10](#) e o processo descrito na [Seção 5.1](#)).

1. O documento JSON do pedido DEVE conter apenas duas chaves: `msg`, associada ao valor 1, e `jwt` (veja [Subseção 6.1.1](#));
2. O `token` JWT é assinado com a [chave privada](#) da SEF correspondente à [chave pública](#) contida no [certificado digital da SEF](#) inserido no DAF (veja [Subseção 6.1.1](#));
 - 2.1. O conteúdo do `token` JWT é apresentado na [Tabela 6.3](#).
3. Em caso de sucesso, o DAF DEVE gerar uma resposta contendo um documento JSON com apenas duas chaves: `res` e `jwt`;
 - 3.1. O `token` JWT DEVE ser assinado com a [chave de ateste](#), cuja [chave pública](#) correspondente deverá estar de forma explícita no cabeçalho do `token`, e terá como conteúdo (*payload*) uma chave `jwt`;
 - 3.1.1. O valor associado a essa chave `jwt` DEVE ser outro `token` JWT, o qual DEVE ser assinado com a [chave privada do DAF](#), cuja [chave pública](#) correspondente deverá estar de forma explícita no cabeçalho do `token`, e ter como conteúdo as informações apresentadas na [Tabela 6.4](#).
4. Em caso de insucesso, o DAF DEVE gerar uma das seguintes respostas: `estadoIncorreto` (1), `pedidoMalFormado` (2) ou `assinaturaInvalida` (3). As descrições das respostas de erro podem ser encontradas na [Tabela 6.2](#).

Tabela 6.3: Informações encaminhadas no pedido registrar

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
<code>nnc</code>	22	<i>string</i>	Valor aleatório gerado pela SEF representado em Base64URL

Tabela 6.4: Informações encaminhadas na resposta do pedido registrar

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
daf	22	<i>string</i>	Identificador único do DAF representado em Base64URL
cnt	4	inteiro	Valor atual do contador monotônico
nnc	22	<i>string</i>	Valor aleatório gerado pela SEF representado em Base64URL

6.1.2.2 confirmarRegistro

Esse pedido é enviado pelo PAF para confirmar o registro do DAF junto à SEF (veja [Caso de Uso UC-4.10](#) e o processo descrito na [Seção 5.1](#)).

1. O documento JSON do pedido DEVE conter apenas duas chaves: `msg`, associada ao valor 2, e `jwt` (veja [Subseção 6.1.1](#));
2. O *token* JWT é assinado com a [chave privada](#) da SEF correspondente à [chave pública](#) contida no [certificado digital da SEF](#) inserido no DAF;
 - 2.1. O conteúdo do *token* JWT é apresentado na [Tabela 6.5](#).
 - 2.2. O valor associado à chave `chs`, quando a [chave SEF](#) for cifrada com o esquema de cifragem RSAES-OAEP, DEVE:
 - 2.2.1. Ser a saída do processo de cifragem da [chave SEF](#) com a chave pública RSA do DAF, representada em Base64URL.
 - 2.3. O valor associado à chave `chs`, quando a [chave SEF](#) for cifrada com o esquema de cifragem ECIES, DEVE:
 - 2.3.1. Utilizar a chave pública EC do DAF para gerar a chave secreta, a ser utilizada no processo de cifragem, com o algoritmo AES-128-CBC-HMAC-SHA-256 ([JONES, 2018](#));
 - 2.3.2. Representar à cifragem da [chave SEF](#) na forma de um *token JSON Web Encryption (JWE)* ([JONES, 2015a](#)) e o *header* do JWE DEVE possuir as chaves `alg`, `enc` e `epk`;
 - 2.3.2.1. O valor associado à chave `alg` DEVE ser ECDH-ES;
 - 2.3.2.2. O valor associado à chave `enc` DEVE ser A128CBC-HS256;
 - 2.3.2.3. O valor associado à chave `epk` DEVE ser um documento JSON, que por sua vez DEVE possuir as chaves `crv`, `kty`, `x` e `y` (veja exemplo na [Seção A.7](#));
3. Em caso de sucesso, o DAF DEVE gerar uma resposta de sucesso (0) sem parâmetros;
4. Em caso de insucesso, o DAF DEVE gerar uma das seguintes respostas: `pedidoMalFormado` (2) ou `assinaturaInvalida` (3). As descrições das respostas de erro podem ser encontradas na [Tabela 6.2](#);

6.1.2.3 solicitarAutenticacao

Esse pedido é enviado pelo PAF para receber um *nonce* gerado pelo DAF (veja o [Caso de Uso UC-4.6](#) e o processo descrito na [Seção 5.2](#)).

Tabela 6.5: Informações encaminhadas no pedido `confirmarRegistro`

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
<code>chs</code>	variável	<i>string</i>	Chave SEF cifrada
<code>chp</code>	86	<i>string</i>	Chave PAF representada em Base64URL
<code>mop</code>	1	inteiro	Modo de operação do DAF. DEVE ser 0 quando o DAF não for compartilhado entre PDVs e DEVE ser 1 quando DAF for compartilhado entre PDVs

1. O pedido não possui parâmetros e o documento JSON do pedido DEVE conter apenas a chave `msg` associada ao valor 3;
2. Em caso de sucesso, O DAF DEVE gerar uma resposta de sucesso (0) com os parâmetros apresentados na Tabela 6.6;
3. Em caso de insucesso, o DAF DEVE gerar uma resposta de `estadoIncorreto` (1) ou `pedidoMalFormado` (2). A Tabela 6.2 apresenta a descrição desse erro.

Tabela 6.6: Informações encaminhadas na resposta do pedido `solicitarAutenticacao`

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
<code>nnc</code>	22	<i>string</i>	Valor aleatório gerado pelo DAF representado em Base64URL

6.1.2.4 autorizarDFE

Esse pedido é enviado pelo PAF para solicitar autorização sobre um DF-e (veja o Caso de Uso UC-4.6 e o processo descrito na Seção 5.2).

1. O documento JSON do pedido DEVE conter a chave `msg`, associada ao valor 4, e lista de parâmetros conforme apresentado na Tabela 6.7;
2. Em caso de sucesso, O DAF DEVE gerar um documento JSON com apenas duas chaves: `res`, associada com o valor 0, e `jwt`;
 - 2.1. O `token` JWT DEVE ter sua integridade e autenticidade garantida por meio de uma função HMAC-SHA256 que teve como chave a chave SEF;
 - 2.2. O conteúdo do `token` JWT é apresentado na Tabela 6.8.
3. Em caso de insucesso, o DAF DEVE gerar uma das seguintes respostas: `estadoIncorreto` (1), `pedidoMalFormado` (2) ou `pafDesconhecido` (4). A Tabela 6.2 apresenta a descrição destes erros.

Tabela 6.7: Informações encaminhadas no pedido `autorizarDFE`

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
<code>fdf</code>	variável	<i>string</i>	Documento XML com as informações essenciais do DF-e codificado em Base64URL
<code>hdf</code>	43	<i>string</i>	Resumo criptográfico do DF-e completo representado em Base64URL

pdv	10	string	Identificador único do PDV
red	43	string	Saída de uma função HMAC representada em Base64URL (veja Caso de Uso UC-4.6)

Tabela 6.8: Informações encaminhadas na resposta do pedido `autorizarDFE`

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
daf	22	string	Identificador único do DAF representado em Base64URL
vsb	1	inteiro	Versão atual do software básico
mop	1	inteiro	Modo de operação do DAF. DEVE ser 0 quando o DAF não for compartilhado entre PDVs e DEVE ser 1 quando DAF for compartilhado entre PDVs
pdv	10	string	Identificador único do PDV
cnt	4	inteiro	Valor atual do contador monotônico
aut	43	string	Identificador único da autorização DAF representado em Base64URL

6.1.2.5 `apagarAutorizacaoRetida`

Esse pedido é enviado pelo PAF para remover uma autorização retida na MT do DAF (veja o [Caso de Uso UC-4.2](#) e o processo descrito na [Seção 5.3](#)).

1. O pedido DEVE conter a chave `msg`, associada ao valor 5, e a lista de parâmetros conforme apresentado na [Tabela 6.9](#);
2. Em caso de sucesso, o DAF DEVE gerar uma resposta de sucesso (0) sem parâmetros;
3. Em caso de insucesso, o DAF DEVE gerar uma das seguintes respostas: `estadoIncorreto` (1), `pedidoMalFormado` (2), `hmacNaoCorrespondente` (5) ou `autorizacaoNaoEncontrada` (6). As descrições das respostas de erro podem ser encontradas na [Tabela 6.2](#).

Tabela 6.9: Informações encaminhadas no pedido `apagarAutorizacaoRetida`

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
aut	43	string	Identificador único da autorização DAF representado em Base64URL
apg	43	string	Saída de uma função HMAC representada em Base64URL que teve como chave a chave SEF e como pedido o <code>idAut</code>

6.1.2.6 `removerRegistro`

Esse pedido é enviado pelo PAF para iniciar o processo de remoção de registro de um DAF que fora previamente registrado junto a SEF (veja o [Caso de Uso UC-4.11](#) e o processo descrito na [Seção 5.5](#)).

1. O documento JSON do pedido DEVE conter apenas duas chaves: `msg`, associada ao valor 6, e `jwt` (veja [Subseção 6.1.1](#));
2. O `token` JWT é assinado com a [chave privada](#) da SEF correspondente à [chave pública](#) contida no [certificado digital da SEF](#) inserido no DAF;
 - 2.1. O conteúdo do `token` JWT é apresentado na [Tabela 6.10](#).

3. Em caso de sucesso, o DAF DEVE gerar uma resposta contendo um documento JSON com apenas duas chaves: `res` e `jwt`;
- 3.1. O `token` JWT DEVE ser assinado com a [chave privada do DAF](#) e terá como conteúdo (`payload`) os parâmetros apresentados na [Tabela 6.11](#).
4. Em caso de insucesso, o DAF DEVE gerar uma das seguintes respostas: `estadoIncorreto` (1), `pedidoMalFormado` (2), `assinaturaInvalida` (3) OU `autorizacaoRetida` (7). As descrições das respostas de erro podem ser encontradas na [Tabela 6.2](#).

Tabela 6.10: Informações encaminhadas no pedido `removeRegistro`

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
<code>nnc</code>	22	<i>string</i>	Valor aleatório gerado pela SEF representado em Base64URL

Tabela 6.11: Informações encaminhadas na resposta do pedido `removeRegistro`

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
<code>daf</code>	22	<i>string</i>	Identificador único do DAF representado em Base64URL
<code>cnt</code>	4	inteiro	Valor atual do contador monotônico
<code>nnc</code>	22	<i>string</i>	Valor aleatório gerado pela SEF representado em Base64URL

6.1.2.7 `confirmarRemocaoRegistro`

Esse pedido é enviado pelo PAF para finalizar o processo de remoção de registro do DAF junto a SEF que fora previamente iniciado (veja o [Caso de Uso UC-4.11](#) e o processo descrito na [Seção 5.5](#)).

1. O documento JSON do pedido DEVE conter apenas duas chaves: `msg`, associada ao valor 7, e `jwt` (veja [Subseção 6.1.1](#));
2. O `token` JWT é assinado com a [chave privada da SEF](#) correspondente à [chave pública](#) contida no [certificado digital da SEF](#) inserido no DAF;
 - 2.1. O conteúdo do `token` JWT é apresentado na [Tabela 6.12](#).
3. Em caso de sucesso, o DAF DEVE gerar uma resposta de sucesso (0) sem parâmetros;
4. Em caso de insucesso, o DAF DEVE gerar uma das seguintes respostas: `pedidoMalFormado` (2) OU `assinaturaInvalida` (3). As descrições das respostas de erro podem ser encontradas na [Tabela 6.2](#).

Tabela 6.12: Informações encaminhadas no pedido `confirmarRemocaoRegistro`

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
<code>evn</code>	7	<i>string</i>	Cadeia de caracteres REMOVE

6.1.2.8 `consultarInformacoes`

Esse pedido é enviado pelo PAF ou pelo Aplicativo Fisco para obter informações sobre o DAF (veja o [Caso de Uso UC-4.7](#)).

1. O pedido não possui parâmetros e o documento JSON do pedido DEVE conter apenas a chave `msg` associada ao valor 8;
2. Em caso de sucesso, o DAF DEVE gerar uma resposta de `sucesso` (0) com os parâmetros apresentados na [Tabela 6.13](#);
3. Em caso de insucesso, o DAF DEVE gerar uma resposta de `estadoIncorreto` (1) ou `pedidoMalFormado` (2). A [Tabela 6.2](#) apresenta a descrição desse erro.

Tabela 6.13: Informações encaminhadas na resposta do pedido `consultarInformacoes`

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
<code>daf</code>	22	<i>string</i>	Identificador único do DAF representado em Base64URL
<code>mop</code>	1	inteiro	Modo de operação do DAF. DEVE ser 0 quando o DAF não for compartilhado entre PDVs e DEVE ser 1 quando DAF for compartilhado entre PDVs
<code>vsb</code>	1	inteiro	Versão atual do software básico
<code>hsb</code>	43	<i>string</i>	Resumo criptográfico do software básico representado em Base64URL
<code>fab</code>	14	<i>string</i>	Representação em <i>string</i> do CNPJ do fabricante do DAF (somente os números)
<code>mdl</code>	1-20	<i>string</i>	Modelo do DAF
<code>cnt</code>	4	inteiro	Valor atual do contador monotônico
<code>crt</code>	variável	<i>string</i>	Certificado digital da SEF codificado no formato textual PEM de acordo com Josefsson e Leonard (2015)
<code>est</code>	variável	<i>string</i>	Estado atual do DAF
<code>mxd</code>	4	inteiro	Limite máximo de autorizações que o DAF é capaz de reter em memória. O menor valor entre as condições de guarda <code>maxDFeSeF</code> , definido pela SEF, e <code>maxDFeModel</code> , definido pelo fabricante e relacionado com o tamanho da memória do dispositivo
<code>ndf</code>	4	inteiro	Condição de guarda <code>numDFe</code> . Quantidade de autorizações retidas no DAF
<code>rts</code>	variável	<i>array</i>	Vetor com Identificadores únicos das autorizações

6.1.2.9 atualizarSB

Esse pedido é enviado pelo PAF para que o DAF se prepare para iniciar o processo de atualização de SB (veja o [Caso de Uso UC-4.5](#) e o processo descrito na [Seção 5.6](#)).

1. O pedido não possui parâmetros e o documento JSON do pedido DEVE conter apenas a chave `msg` associada ao valor 9;
2. Em caso de sucesso, o DAF DEVE gerar uma resposta de `sucesso` (0) sem parâmetros;
3. Em caso de insucesso, o DAF DEVE gerar uma das seguintes respostas: `estadoIncorreto` (1), `pedidoMalFormado` (2) ou `autorizacaoRetida` (7). As descrições das respostas de erro podem ser encontradas na [Tabela 6.2](#).

6.1.2.10 atualizarCertificado

Esse pedido é enviado pelo PAF para atualizar o [certificado digital da SEF](#) armazenado no DAF (veja o [Caso de Uso UC-4.4](#) e o processo descrito na [Seção 5.7](#)).

1. O documento JSON do pedido DEVE conter a chave `msg`, associada ao valor 10, e lista de parâmetros conforme apresentado na [Tabela 6.14](#);
2. Em caso de sucesso, o DAF DEVE gerar uma resposta de sucesso (0) sem parâmetros;
3. Em caso de insucesso, o DAF DEVE gerar uma das seguintes respostas: `estadoIncorreto` (1), `pedidoMalFormado` (2), `assinaturaInvalida` (3) ou `autorizacaoRetida` (7). A [Tabela 6.2](#) apresenta a descrição desses erros.

Tabela 6.14: Informações encaminhadas no pedido `atualizarCertificado`

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
<code>crt</code>	variável	<i>string</i>	Certificado digital da SEF codificado no formato textual PEM de acordo com Josefsson e Leonard (2015)

6.1.2.11 `descarregarRetido`

Esse pedido é enviado pelo PAF ou pelo aplicativo fisco para que o DAF descarregue detalhes de uma autorização retida em sua MT (veja o [Caso de Uso UC-4.9](#)).

1. O documento JSON do pedido DEVE conter a chave `msg`, associada ao valor 11, e lista de parâmetros conforme apresentado na [Tabela 6.15](#);
2. Em caso de sucesso, o DAF DEVE gerar uma resposta de sucesso (0) com os parâmetros apresentados na [Tabela 6.16](#);
3. Em caso de insucesso, o DAF DEVE gerar uma das seguintes respostas: `estadoIncorreto` (1), `pedidoMalFormado` (2) ou `autorizacaoNaoEncontrada` (6). A [Tabela 6.2](#) apresenta a descrição desses erros.

Tabela 6.15: Informações encaminhadas no pedido `descarregarRetido`

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
<code>aut</code>	43	<i>string</i>	Identificador único da autorização DAF representado em Base64URL

Tabela 6.16: Informações encaminhadas na resposta do pedido `descarregarRetido`

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
<code>jwt</code>	variável	<i>string</i>	Token JWT com a autorização do DF-e, cujo conteúdo é apresentado na Tabela 6.8
<code>fdf</code>	variável	<i>string</i>	Documento XML com as informações essenciais do DF-e codificado em Base64URL
<code>hdf</code>	43	<i>string</i>	Resumo criptográfico do DF-e completo representado em Base64URL

6.1.2.12 `alterarModoOperacao`

Esse pedido é enviado pelo PAF para iniciar o processo de alteração do modo de operação do DAF (veja o [Caso de Uso UC-4.1](#) e o processo descrito na [Seção 5.8](#)).

1. O documento JSON do pedido DEVE conter apenas duas chaves: `msg`, associada ao valor 12, e `jwt` (veja [Subseção 6.1.1](#));
2. O `token` JWT DEVE ter sua integridade e autenticidade garantida por meio de uma função HMAC-SHA256 que teve como chave a `chave SEF`;
 - 2.1. O conteúdo do `token` JWT é apresentado na [Tabela 6.17](#).
3. Em caso de sucesso, o DAF DEVE gerar uma resposta contendo um documento JSON com apenas duas chaves: `res` e `jwt`;
 - 3.1. O `token` JWT DEVE ter sua integridade e autenticidade garantida por meio de uma função HMAC-SHA256 que teve como chave a `chave SEF` e terá como conteúdo (`payload`) os parâmetros apresentados na [Tabela 6.18](#).
4. Em caso de insucesso, o DAF DEVE gerar uma das seguintes respostas: `estadoIncorreto` (1), `pedidoMalFormado` (2), `hmacNaoCorrespondente` (5) ou `autorizacaoRetida` (7). As descrições das respostas de erro podem ser encontradas na [Tabela 6.2](#).

Tabela 6.17: Informações encaminhadas no pedido `alterarModoOperacao`

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
<code>nnc</code>	22	<i>string</i>	Valor aleatório gerado pela SEF representado em Base64URL

Tabela 6.18: Informações encaminhadas na resposta do pedido `alterarModoOperacao`

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
<code>daf</code>	22	<i>string</i>	Identificador único do DAF representado em Base64URL
<code>cnt</code>	4	inteiro	Valor atual do contador monotônico
<code>nnc</code>	22	<i>string</i>	Valor aleatório gerado pela SEF representado em Base64URL

6.1.2.13 `confirmarAlterarModoOperacao`

Esse pedido é enviado pelo PAF para finalizar o processo de alteração do modo de operação do DAF que fora previamente iniciado (veja o [Caso de Uso UC-4.1](#) e o processo descrito na [Seção 5.8](#)).

1. O documento JSON do pedido DEVE conter apenas duas chaves: `msg`, associada ao valor 13, e `jwt` (veja [Subseção 6.1.1](#));
2. O `token` JWT DEVE ter sua integridade e autenticidade garantida por meio de uma função HMAC-SHA256 que teve como chave a `chave SEF`;
 - 2.1. O conteúdo do `token` JWT é apresentado na [Tabela 6.19](#).
3. Em caso de sucesso, o DAF DEVE gerar uma resposta de sucesso (0) sem parâmetros;
4. Em caso de insucesso, o DAF DEVE gerar uma das seguintes respostas: `pedidoMalFormado` (2) ou `hmacNaoCorrespondente` (5). As descrições das respostas de erro podem ser encontradas na [Tabela 6.2](#).

Tabela 6.19: Informações encaminhadas no pedido `confirmarAlterarModoOperacao`

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
<code>mop</code>	1	inteiro	Modo de operação do DAF. DEVE ser 0 quando o DAF não for compartilhado entre PDVs e DEVE ser 1 quando DAF for compartilhado entre PDVs

6.1.2.14 `cancelarProcesso`

Esse pedido é enviado pelo PAF para que o DAF cancele qualquer processo ou caso de uso que tenha sido iniciado previamente.

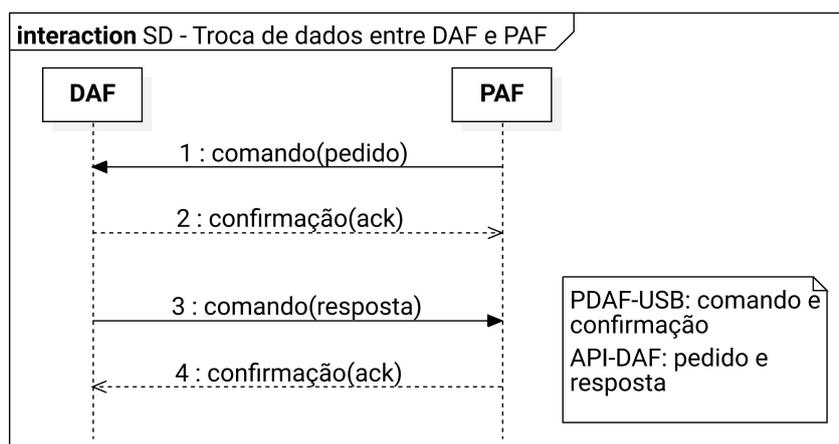
1. O pedido não possui parâmetros e o documento JSON do pedido DEVE conter apenas a chave `msg` associada ao valor 14;
2. Em caso de sucesso, o DAF DEVE gerar uma resposta de `sucesso` (0) sem parâmetros;
3. Em caso de insucesso, o DAF DEVE gerar uma resposta de `estadoIncorreto` (1). A Tabela 6.2 apresenta a descrição desse erro.

6.2 Protocolo DAF-USB

Na Seção 3.6 são apresentados os requisitos estruturais da interface `USB` do DAF e de padronização para garantir a interoperabilidade entre DAFs e PAFs de diferentes fabricantes. Nesta seção são definidos os detalhes para o transporte das pedidos e respostas da API DAF (ver Seção 6.1) via interface `USB`.

Enquanto a API DAF foi projetada para ser independente da interface de comunicação utilizada pelo DAF, o Protocolo DAF-USB (PDAF-USB) foi projetado para operar especificamente com a interface `USB`. A API DAF é baseada em pedido e resposta, enquanto o PDAF-USB é um protocolo de comunicação do tipo `pare-e-espere`, ou seja, cada comando trocado entre DAF e PAF deve ter uma confirmação de entrega (`ACK`). Dessa forma, neste documento é usada a nomenclatura `pedido-resposta` para se referir à API DAF e os elementos `comando-confirmação` para se referir ao PDAF-USB. Na Figura 6.1 é apresentada a sequência de comunicação da API DAF encapsulada e transportada pela interface `USB` utilizando o esquema de `comando-confirmação` do PDAF-USB.

Figura 6.1: Sequência de pedido-resposta da API DAF encapsulada pelo PDAF-USB



O **PDAF-USB** define os comandos-confirmação e o formato do quadro dos comandos. A implementação do protocolo é dividida em duas subcamadas: i) **Garantia de entrega**, serviço responsável por garantir ao transmissor que um comando foi entregue ou não ao destino; ii) **Enquadramento**, responsável pelo encapsulamento dos pedidos ou respostas da API DAF. Na [Figura 6.2](#) é apresentada a disposição do **PDAF-USB** no cenário de comunicação, bem como a estrutura do quadro e da organização das subcamadas de serviço.

Os comandos disponíveis para transportar as pedidos ou respostas da API DAF são apresentados na [Tabela 6.20](#). Esses comandos identificam o tipo do conteúdo transportado pelo **PDAF-USB** e são detalhados, juntamente com as confirmações, na [Subseção 6.2.4](#).

1. O DAF DEVE implementar todos os comandos apresentados na [Tabela 6.20](#);
2. O DAF NÃO DEVE implementar nenhum outro comando exclusivo do fabricante.

Figura 6.2: Organização hierárquica da comunicação do **PDAF-USB**

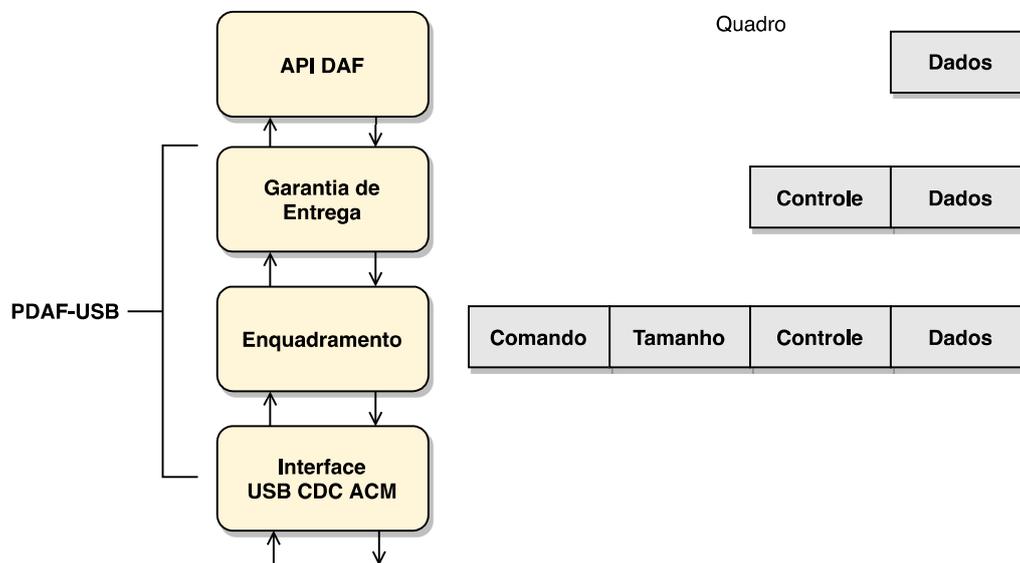


Tabela 6.20: Comandos de transporte do **PDAF-USB**

Nome do comando	Valor	Descrição
enviarMensagem	0x01	Envia um pedido ou resposta da API DAF. Também é utilizado para envio da confirmação (ACK) no PDAF-USB
enviarBinário	0x02	Envia dados brutos (<i>raw data</i>)

6.2.1 Formato do quadro do **PDAF-USB**

Na [Tabela 6.21](#) é apresentado o formato do quadro do **PDAF-USB**. Esse formato DEVE ser utilizado nos envios dos comandos e da confirmação (veja [Subseção 6.2.4](#)).

Tabela 6.21: Formato do quadro **PDAF-USB**

Nome do campo	Tamanho (<i>bytes</i>)	Descrição
Comando	1	Código do comando dependendo do tipo de dados (veja Tabela 6.20)

Tamanho	2 ou 4	Soma dos tamanhos dos campos <code>Controle</code> e <code>Dados</code> . Valor deverá ser representado em <i>big-endian</i>
Controle	1	Código de controle para garantia de entrega, conforme detalhado na Subseção 6.2.2
Dados	0 a $(2^N - 2)$	Dados transmitidos; $N = \text{Tamanho do campo Tamanho} \times 8$

6.2.2 Garantia de entrega

A comunicação **PDAF-USB** é do tipo *pare-e-espere* de forma que, cada comando trocado entre **DAF** e **PAF** DEVE haver uma confirmação de entrega desse comando. A subcamada **Garantia de entrega** DEVE adicionar, ao quadro que será transmitido, o campo `Controle`, o qual DEVE conter um dos valores apresentados na [Tabela 6.22](#). Caso ocorram perdas de pacote, o sincronismo é garantido por meio de retransmissões baseadas nos números de sequência com valores 0 ou 1 no campo `Controle`. Durante a recepção, o número de sequência bem como o tipo do conteúdo do campo `Controle` devem ser verificados a fim de garantir que a subcamada **Garantia de entrega** receba o comando esperado e realize retransmissões, se necessário.

Tabela 6.22: Códigos de controle da subcamada Garantia de entrega do PDAF-USB

Tipo de conteúdo	Valor	Descrição
DATA_0	0x00	Indica que é um quadro de dados com sequência zero
DATA_1	0x08	Indica que é um quadro de dados com sequência um
ACK_0	0x80	Confirmação do recebimento de um quadro com sequência zero
ACK_1	0x88	Confirmação do recebimento de um quadro com sequência um



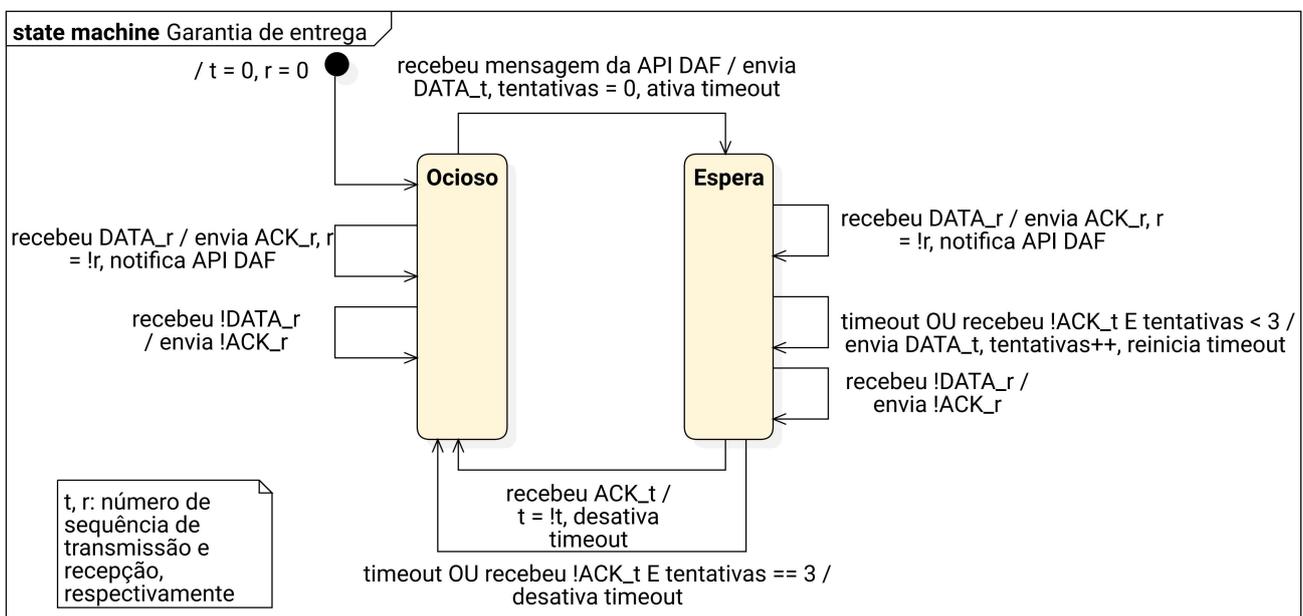
O PAF DEVE realizar retransmissões dos pedidos da API DAF para sincronizar os códigos de controle antes de considerar que o DAF está inalcançável.

Na [Figura 6.3](#) é apresentada a modelagem dos processos de recepção e transmissão da subcamada de Garantia de entrega e no [Apêndice C](#) são apresentados pseudocódigos de referência. O comportamento da subcamada é descrito da seguinte forma:

- Transmissão:
 1. O primeiro comando a ser enviado DEVE conter o campo `Controle` igual a `DATA_0`;
 2. Após a montagem do quadro, a subcamada Garantia de entrega DEVE enviar para a subcamada Enquadramento o quadro montado e o valor do campo `Comando` definido pela API DAF;
 3. Após a transmissão de um comando, DEVE ser realizada a troca do estado `0cioso` para o estado `Espera`;
 4. No estado `Espera`, a subcamada DEVE aguardar a recepção de um `ACK`;
 - 4.1. Em caso de sucesso, DEVE retornar para o estado `0cioso`;
 - 4.2. Em caso de *timeout*, o comando DEVE ser retransmitido;
 - 4.3. Em caso de atingir limite de tentativas, retorna para o estado `0cioso`.

5. Antes de realizar o envio de um novo comando, DAF e PAF DEVEM receber um ACK para ter a garantia que um comando completo foi recebido pela outra parte;
 6. O tempo máximo para receber um ACK DEVE ser de 1 segundo;
 7. O número máximo de tentativas de retransmissão DEVE ser igual a três.
- Recepção:
 8. O protocolo DEVE ser capaz de receber um conteúdo do tipo DATA e responder com ACK indiferente do estado que ele esteja;
 9. Após a recepção de um quadro completo, a subcamada Garantia de entrega DEVE enviar para a API DAF o campo Dados recebido.

Figura 6.3: Máquina de estados da Garantia de entrega



6.2.3 Enquadramento

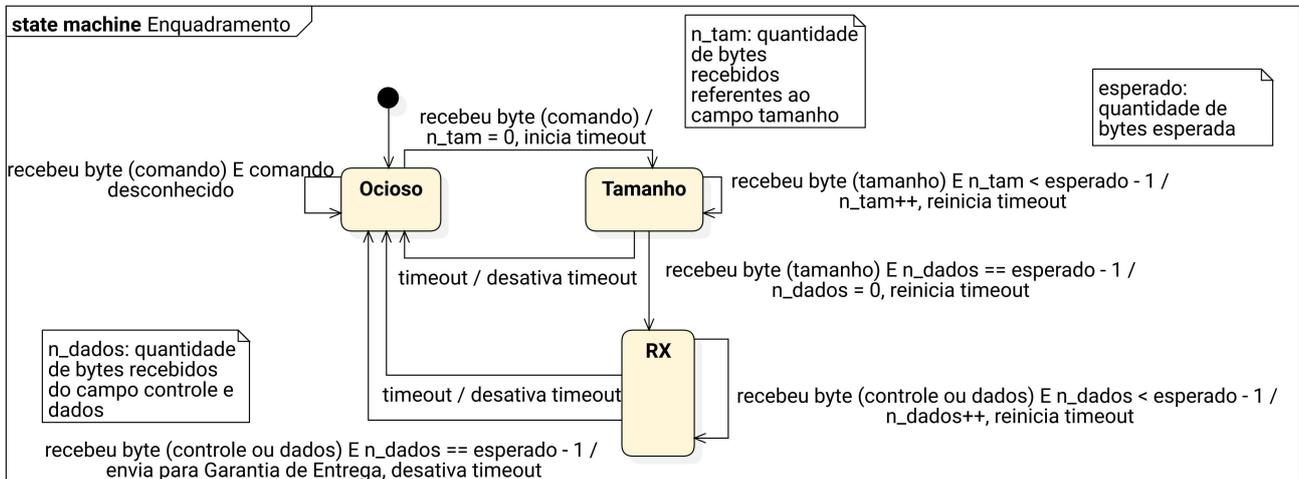
A subcamada de Enquadramento é responsável por identificar e delimitar quadros por meio da contagem de caracteres. Para isso, utilizam-se dois campos: Comando e Tamanho. Durante a transmissão esses campos devem ser adicionados ao quadro recebido da subcamada superior.

Na recepção de comandos, a subcamada de Enquadramento é definida a partir de uma máquina de estados finitos apresentada na Figura 6.4. Pseudocódigos de referência são apresentados no Apêndice C. O comportamento da subcamada é descrito da seguinte forma:

1. O primeiro estado da subcamada de Enquadramento DEVE ser o Ocioso;
2. Ao receber o primeiro *byte*, a subcamada Enquadramento DEVE verificar se o valor é um dos apresentados na Tabela 6.20;
 - 2.1. Em caso de sucesso, a subcamada DEVE ir para o estado Tamanho;
 - 2.2. Em caso de insucesso, a subcamada se mantém no estado Ocioso;
3. O tempo limite até a recepção de um novo *byte* DEVE ser de 500 milissegundos.

4. Ao finalizar a recepção dos *bytes* referentes ao tamanho da informação recebida, a subcamada DEVE ir para o estado RX;
5. Após a recepção de um quadro completo, a subcamada Enquadramento DEVE enviar para a subcamada Garantia de entrega o campo *Comando* e os *bytes* recebidos no estado RX;

Figura 6.4: Máquina de estados da recepção do Enquadramento



6.2.4 Detalhamento dos comandos e confirmação do PDAF-USB

Esta seção detalha os comandos `enviarMensagem` e `enviarBinario` e a confirmação do **PDAF-USB** apresentando na [Tabela 6.20](#). Na [Tabela 6.23](#) é apresentado o formato do comando `enviarMensagem`, o qual DEVE ser utilizado para o transporte de todos os pedidos e respostas da API DAF (veja [Subseção 6.1.2](#)).

Tabela 6.23: Quadro do comando `enviarMensagem`

Nome do campo	Tamanho (bytes)	Valor
Comando	1	0x01
Tamanho	2	Soma dos tamanhos dos campos Controle e Dados; Valor entre 1 e $(2^{16} - 1)$
Controle	1	Código de controle DATA (veja Subseção 6.2.2).
Dados	variável	Pedido ou resposta da API DAF (JSON)

Na [Tabela 6.24](#) é apresentado o formato do comando `enviarBinario`, o qual DEVE ser utilizado exclusivamente para o transporte de dados brutos (*raw data*) que formam o arquivo contendo a imagem de atualização do **SB** (veja [Caso de Uso UC-4.5](#)).

Tabela 6.24: Quadro do comando `enviarBinario`

Nome do campo	Tamanho (bytes)	Valor
Comando	1	0x02
Tamanho	4	Soma dos tamanhos dos campos Controle e Dados; Valor entre 1 e $(2^{32} - 1)$
Controle	1	Código de controle DATA (veja Subseção 6.2.2)
Dados	variável	Dados brutos (<i>raw data</i>)

Na [Tabela 6.25](#) é apresentado o formato da confirmação, em caso de sucesso, dos comandos `enviarMensagem` e `enviarBinario`.

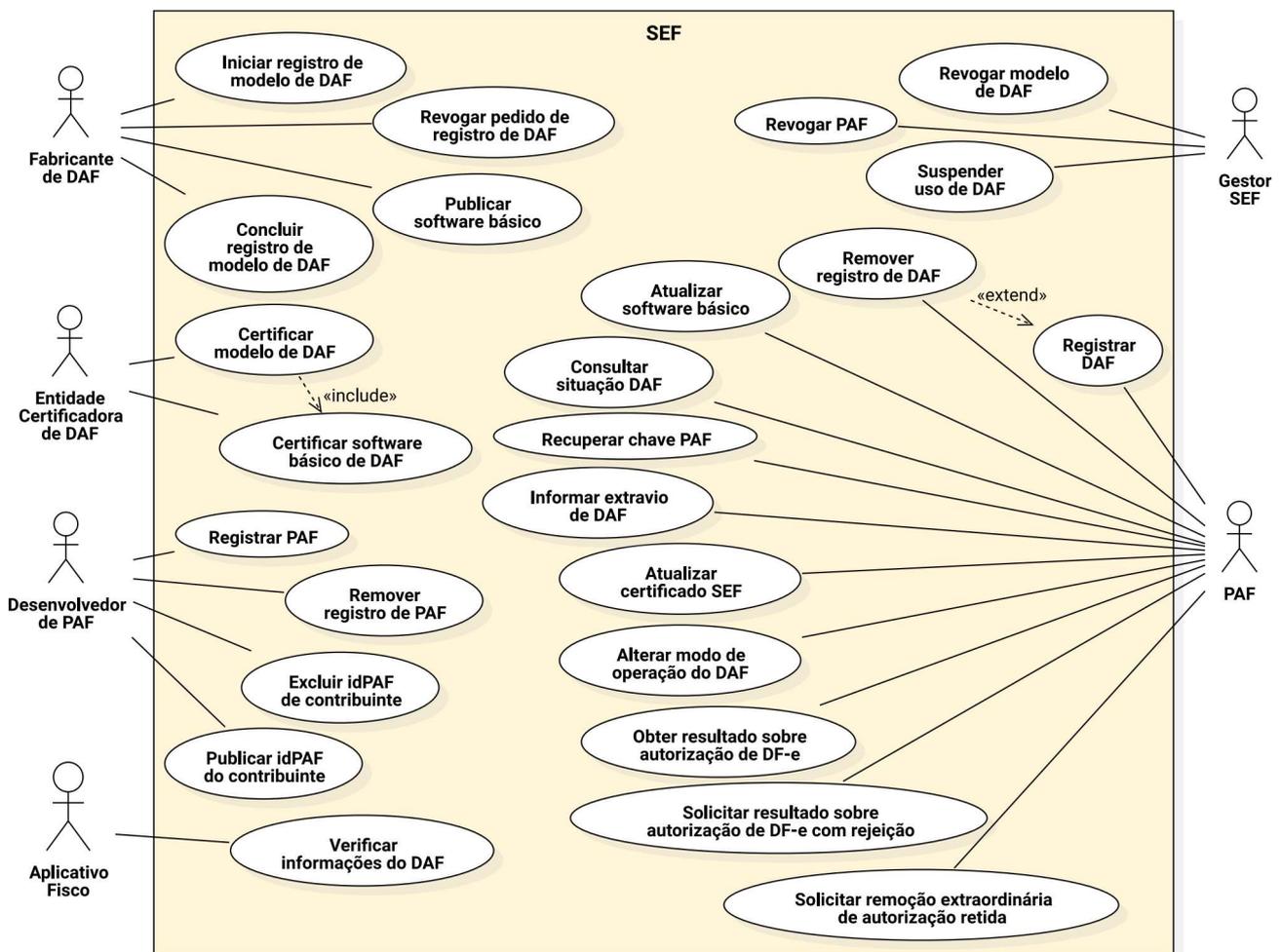
Tabela 6.25: Quadro da confirmação dos comandos `enviarMensagem` e `enviarBinario`

Nome do campo	Tamanho (<i>bytes</i>)	Valor
Comando	1	0x01
Tamanho	2	0x0001
Controle	1	Código de controle ACK (veja Subseção 6.2.2)
Dados	0	Vazio

7 Serviços providos pela SEF

Nesse capítulo são apresentados, por meio de cenários de uso, todos os serviços ofertados pela Secretaria de Estado da Fazenda de Santa Catarina para o projeto DAF. Na Figura 7.1 é ilustrado um diagrama de casos de uso UML com os serviços providos pela SEF para cada ator, sendo esses: PAF, fabricantes de DAF, desenvolvedores de PAF, entidades certificadoras de DAF, auditor fiscal e o próprio Fisco.

Figura 7.1: Diagrama de caso de uso da SEF



7.1 Processos operacionais para fabricantes de DAF

Nessa seção são apresentados todos os processos operacionais destinados aos fabricantes de DAF. Para os processos aqui apresentados foram assumidas as seguintes premissas:

1. Fabricante de DAF possui e-CNPJ válido;
2. Fabricante de DAF está credenciado junto à SEF.

7.1.1 Iniciar registro de modelo de DAF

Antes que o fabricante possa iniciar a comercialização de um modelo de DAF, esse deve fazer o registro do mesmo junto à SEF. O processo de registro consiste de três fases: (1) início – o fabricante envia a SEF informações sobre o modelo e a **chave pública** par da **chave privada** que será usada como a **chave de ateste** desse modelo; (2) certificação do modelo – o modelo é submetido a uma entidade certificadora credenciada para que essa ateste que o modelo está de acordo com as especificações; (3) conclusão – o fabricante informa a SEF que o modelo foi certificado e solicita autorização para iniciar a comercialização do mesmo.

Nessa seção são apresentados detalhes sobre a primeira fase do processo de registro. O fabricante deve fornecer informações sobre o modelo de DAF por meio de uma **solicitação de assinatura de certificado – Certificate Signing Request (CSR)** – de acordo com a especificação PKCS #10 (NYSTROM; KALISKI, 2000). O par de chaves e o CSR devem ser gerados pelo fabricante e são exclusivos para um único modelo de DAF, não podendo de forma alguma serem reutilizados em outros modelos. A **chave privada**, usada para gerar o CSR, será então a **chave de ateste** deste modelo de DAF e cabe ao fabricante garantir o total sigilo sobre a mesma. Se a **chave de ateste** for comprometida, então o modelo de DAF será revogado pela SEF e não poderá ser usado para autorizar DF-e. Na **Tabela 7.1** são listados os campos que deverão estar presentes no CSR.

Tabela 7.1: Descrição dos campos do CSR para registro de modelo de DAF

Campo	Descrição
Country (C)	Sigla do país. Preencher com a sequência “BR”
State (ST)	Nome por extenso do estado onde a sede da fabricante está situada
Locality (L)	Nome por extenso da cidade onde a sede da fabricante está situada
Organization (O)	Razão social da fabricante igual ao existente no registro CNPJ
Common Name (CN)	Nome único do modelo concatenado com o CNPJ do fabricante, sem os caracteres de pontuação, e separado pelo caractere “:”. Por exemplo: ModeloArev1:XXXXXXXXYYYYZZ
OID=2.16.76.1.3.3 (CNPJ)	CNPJ do fabricante, sem os caracteres de pontuação

Neste caso a SEF atuará com uma **Autoridade Certificadora (AC)** exclusiva para emissão de certificados para modelos de DAF de acordo com a especificação (COOPER et al., 2008). A SEF, ao verificar que o pedido está correto, persiste em sua base os dados do modelo de DAF extraídos da CSR, o que inclui a **chave pública**. O fabricante ao receber o certificado digital da SEF estará apto a iniciar o processo de certificação desse modelo de DAF junto a uma entidade certificadora credenciada pela SEF. O certificado digital emitido pela SEF terá um prazo de expiração e se o modelo de DAF não for certificado antes de sua expiração, o fabricante precisará solicitar um novo certificado.

i O processo de emissão de certificado digital pela SEF, aqui descrito, tem como principal objetivo permitir à SEF receber a chave pública par da chave de ateste de um modelo de DAF que o fabricante pretende comercializar. Os certificados digitais emitidos pela SEF são exclusivos para esse fim e podem não estar em conformidade com a [ICP-Brasil](#). Ou seja, a SEF não atua como uma [AC](#) na [ICP-Brasil](#).

7.1.2 Concluir registro de modelo de DAF

Uma vez que um modelo de DAF tenha passado com sucesso pelo processo de acreditação de uma entidade certificadora credenciada pela SEF, o fabricante deverá solicitar à SEF a autorização para que possa iniciar a comercialização desse modelo. Somente após essa etapa que as unidades fabricadas desse modelo de DAF poderão ser usadas para gerar autorizações sobre DF-e.

A SEF manterá, para cada modelo de DAF, informações como: chave pública par da [chave de ateste](#), capacidades criptográficas, versão do [firmware](#) e histórico de versões do [Software Básico \(SB\)](#).

! Qualquer revisão do [hardware](#) ou do [bootloader](#), de um modelo de DAF já registrado, implicará em um novo processo de homologação e o fabricante DEVE realizar o processo descrito na [Subseção 7.1.1](#). Assim, diferentes revisões de um mesmo modelo de DAF terão diferentes [chaves de ateste](#).

7.1.3 Revogar pedido de registro de modelo de DAF

O fabricante pode a qualquer momento solicitar a revogação do processo de registro de um modelo de DAF que ainda não fora concluído. No pedido o fabricante deve informar a razão pela qual está solicitando o cancelamento do registro. Das possíveis razões, pode-se considerar: modelo não passou pelo processo de certificação; alteração do identificador do modelo; desistência da fabricação, etc.

7.1.4 Publicar *software* básico

Diferentes motivos podem gerar a necessidade de uma nova versão de [SB](#) de um modelo de DAF certificado, por exemplo, adequação a uma nova legislação, correção de um comportamento inaquedado, otimização de um comportamento para propiciar um desempenho melhor, etc.

Toda nova versão de [SB](#), antes de ser disponibilizada para os contribuintes, precisará passar pelo processo de certificação junto a uma entidade certificadora credenciada pela SEF. Após isso, o fabricante poderá enviar as informações sobre o novo [SB](#) para a SEF. Dentre as informações que serão fornecidas estará a [URL](#) onde o [SB](#) ficará disponível para que os contribuintes possam baixar, por meio do [PAF](#), e o [resumo criptográfico](#) sobre essa versão do [SB](#) para que o contribuinte possa verificar integridade do arquivo após sua transferência.

A SEF disponibilizará um serviço para que o [PAF](#) possa verificar se existem novas versões de *software* básico para o modelo de DAF com o qual ele interage. Com as informações recebidas o [PAF](#) poderá baixar o novo *software* básico e realizar processo de atualização junto ao seu DAF.

7.2 Processos operacionais para entidades certificadoras de DAF

O processo de certificação a ser seguido pelas entidades certificadoras credenciadas está fora do escopo desse documento e é apresentado em um documento específico. Abaixo é apresentado uma descrição resumida para cada caso de uso.

1. **Certificar modelo de DAF** – Para que uma entidade certificadora credenciada possa atestar que um modelo de DAF está de acordo com as especificações. Após isso, o fabricante de DAF poderá concluir o processo de registro de um modelo de DAF;
2. **Certificar *software* básico de DAF** – Para que uma entidade certificadora credenciada possa atestar que uma nova versão do *software* básico de um modelo de DAF, já certificado, está de acordo com as especificações;

7.3 Processos operacionais para desenvolvedores de PAF

Nessa seção são apresentados todos os processos operacionais destinados aos desenvolvedores de PAF. Para os processos aqui apresentados foram assumidas as seguintes premissas:

1. Desenvolvedor de PAF possui [e-CNPJ](#) válido;
2. Desenvolvedor de PAF possui pelo menos um [Código de Segurança do Responsável Técnico \(CSRT\)](#) ativo junto à [SEF](#);
3. Desenvolvedor de PAF está credenciado junto à [SEF](#).

7.3.1 Registrar PAF

O [PAF](#) deve ser registrado junto à [SEF](#) antes que possa ser usado para operar o DAF. Para registrar, o desenvolvedor do PAF deve informar o identificador do [CSRT](#) que estará associado ao PAF em questão. Esse mesmo [CSRT](#) deverá ser usado pelo desenvolvedor para gerar o [IdPAF](#) de cada [contribuinte](#) que venha a usar esse PAF.

7.3.2 Remover registro de PAF

Caso o desenvolvedor de PAF opte por não mais manter o PAF, e por consequência, não mais comercializá-lo, esse deve remover o registro do mesmo junto à [SEF](#). Assim, terá garantias que nenhum [contribuinte](#) conseguirá registrar novos DAFs para serem operados por um PAF que fora descontinuado. Contudo, isso não afetará àqueles contribuintes que registraram seus DAFs antes da descontinuação do PAF pelo desenvolvedor.

7.3.3 Publicar idPAF de contribuinte

Antes que um [contribuinte](#) possa usar o PAF para operar o DAF, o desenvolvedor do PAF deverá fornecer à [SEF](#) o [IdPAF](#) desse contribuinte. Assim, no processo de registro do DAF (veja [Seção 5.1](#)) a [SEF](#) irá confrontar o [idPAF](#) informado com aquele que já possui em sua base.

7.3.4 Excluir idPAF de contribuinte

Alguns desenvolvedores de PAF podem oferecer modelos de negócio baseado em assinatura para seus clientes, no caso, os contribuintes. Esse serviço permite aos desenvolvedores de PAF informarem ao Fisco que determinado contribuinte não possui mais contrato para utilização de seu PAF.

7.4 Processos operacionais para auditores fiscais da SEF

7.4.1 Verificar informações do DAF

O auditor fiscal da SEF em uma visita *in loco* terá acesso ao DAF do contribuinte e poderá enviar comandos ao mesmo para obter informações como: versão do SB, [resumo criptográfico](#) do SB, [IdDAF](#), modelo, fabricante, número de documentos autorizados, identificadores dos documentos retidos na [Memória de Trabalho \(MT\)](#). O auditor pode então verificar a correspondência dessas informações obtidas do DAF com àquelas mantidas na base do fisco.

7.5 Processos operacionais para o Fisco

7.5.1 Revogar modelo de DAF

A SEF poderá revogar um modelo de DAF certificado caso entenda que o modelo não está de acordo com as diretrizes de segurança, ou mesmo, que não esteja respeitando a legislação. Nesse caso, quando a revogação for efetivada, todos os dispositivos fabricados desse modelo de DAF ficarão impossibilitados de autorizar [DF-e](#).

A SEF atualizará sua base de dados de modelos de DAF e atribuirá o estado de revogado ao referente modelo. Essa situação deverá ser informada ao PAF sempre que esse invocar os serviços providos pela SEF e estiver operando um modelo de DAF revogado.

7.5.2 Revogar PAF

A SEF poderá revogar um [PAF](#) caso entenda que o mesmo não está operando o DAF corretamente, ou mesmo, que não esteja respeitando a legislação. Nesse caso, quando a revogação for efetivada, o PAF estará impossibilitado de invocar os serviços providos pela SEF. A SEF atualizará sua base de dados sobre PAF, atribuindo o estado de revogado e essa situação deverá ser informada ao PAF sempre que esse invocar os serviços providos pela SEF.

7.5.3 Suspender uso de DAF

A SEF poderá suspender o uso de um DAF específico se constatar que o mesmo não está em conformidade com as regras do Fisco. Toda autorização emitida por um DAF suspenso gerará uma exceção por parte da SEF ao PAF. Um DAF suspenso fica impedido de ter seu registro removido pelo PAF. Um DAF só terá sua suspensão cancelada se a SEF puder constatar que o mesmo está em conformidade com as regras do Fisco.

7.6 Processos operacionais para o PAF

Nessa seção são apresentados todos os processos operacionais destinados ao PAF. Para os processos aqui apresentados foram assumidas as seguintes premissas:

1. Contribuinte possui registro junto à SEF e possui e-CNPJ válido;
2. PAF está operando um modelo de DAF certificado pela SEF.
3. PAF possui registro junto à SEF;
4. O desenvolvedor do PAF gerou o **IdPAF**, publicou-o na SEF e entregou-o ao contribuinte;
5. Toda comunicação entre PAF e SEF é feita sobre canais de comunicação seguros (p. ex. TLS (RESCORLA, 2018)).

7.6.1 Registrar DAF

Antes que um DAF possa ser usado para emitir autorizações sobre DF-e, este precisa ser registrado junto à SEF (processo descrito na Seção 5.1). No registro são enviadas as seguintes informações à SEF: características criptográficas do modelo de DAF, informações sobre o PAF que está operando o DAF, informações do contribuinte que está fazendo o registro e o modo de operação do DAF. Após a conclusão do processo de registro de DAF, a base com informações sobre o contribuinte é atualizada de forma a persistir o **IdDAF**, a **chave pública** e o valor atual de seu **contador monotônico** do DAF, bem como a associação desse com o **IdPAF**. Um contribuinte poderá ter vários DAFs registrados. Desta forma, a SEF deve manter as seguintes bases:

1. Modelos de DAF certificados – detalhes sobre o fabricante, detalhes sobre a certificação, características criptográficas, chave pública par da **chave de ateste** e histórico de versões do **Software Básico (SB)**;
2. PAF registrados – detalhes sobre o desenvolvedor e **CSRT** associado a esse;
3. PAF e DAF associados a um contribuinte – para cada par DAF e PAF será persistido também a **chave PAF**, **chave SEF**, **chave pública** do DAF, o último valor conhecido do **contador monotônico** daquele DAF e o valor do **modo de operação do DAF**.

7.6.2 Remover registro de DAF

O contribuinte que não for mais operar com um DAF específico pode remover o registro do mesmo junto à SEF. Esse DAF poderá então ser registrado novamente pelo mesmo contribuinte ou por um outro contribuinte, caso o DAF seja revendido.

Caso o contribuinte queira trocar de fornecedor de PAF, então antes de realizar a troca de PAF, o contribuinte precisará remover o registro do DAF usando o PAF atual. Feito isso, então o contribuinte precisará realizar novamente o processo de registro da DAF, porém dessa vez usando o novo PAF.

7.6.3 Atualizar *software* básico

O PAF poderá questionar se existe uma nova versão do **SB** do DAF que ele opera. No pedido ele informa o **IdPAF**, **IdDAF**, modelo e CNPJ do fabricante do DAF. A SEF retorna informações sobre a última versão de SB disponível para esse modelo, o que inclui: número da versão, data de publicação,

[URL](#) onde a mesma está disponível para ser baixada e [resumo criptográfico](#) sobre o binário dessa versão.

7.6.4 Consultar situação DAF

O PAF poderá verificar como está a situação de seu DAF junto à SEF. O PAF saberá se existe alguma atualização de [SB](#), se o modelo de DAF foi revogado ou mesmo se o DAF em questão foi suspenso pela SEF.

7.6.5 Recuperar chave PAF

Caso o PAF venha a perder a [chave PAF](#), este poderá solicitar à SEF que a envie novamente. O pedido DEVE conter o [IdDAF](#) e ser assinado com o [e-CNPJ](#) do [contribuinte](#).

7.6.6 Informar extravio de DAF

O contribuinte deverá avisar a SEF se ocorrer algum sinistro com o DAF, tal como roubo, extravio ou dano. Futuras autorizações geradas por um DAF extraviado gerará exceção por parte da SEF. Um DAF marcado como extraviado fica impedido de ser usado nos casos de uso de registro (veja [Seção 5.1](#)) e remoção de registro (veja [Seção 5.5](#)).

7.6.7 Atualizar certificado SEF

O modelo de confiança do projeto DAF está fundamentado sobre criptografia de chave pública. As rotinas do DAF que alteram seu estado, como para atualizar de seu [SB](#) ou que visam remover autorizações retidas de sua [MT](#), dependem de comandos enviados pela SEF e assinados com a [chave privada](#) correspondente a [chave pública](#) que está contida no [certificado digital da SEF](#) armazenado no DAF.

Dentro do contexto da [ICP-Brasil](#), certificados digitais possuem um prazo de validade não maior que alguns anos. Sendo assim, quando um certificado expira é necessário que seja emitido um novo e aqueles que dependem desse certificado, como o DAF, devem receber esse novo certificado. A emissão de um novo certificado, contendo uma nova chave privada, possibilitaria também a rolagem periódica de chaves.

O PAF DEVE estar ciente da data de expiração do [certificado digital da SEF](#) contido em seu DAF e antes que esse expire, DEVE realizar o procedimento para substituir esse certificado.

A SEF manterá seus certificados por um período além do prazo de expiração. Isso permitirá a um DAF, que tenha [certificado digital da SEF](#) expirado, instalar um novo [certificado digital da SEF](#). Contudo, um DAF com certificado expirado não poderá participar de processos relacionados com registro de DAF, remoção de registro e atualização de [SB](#).

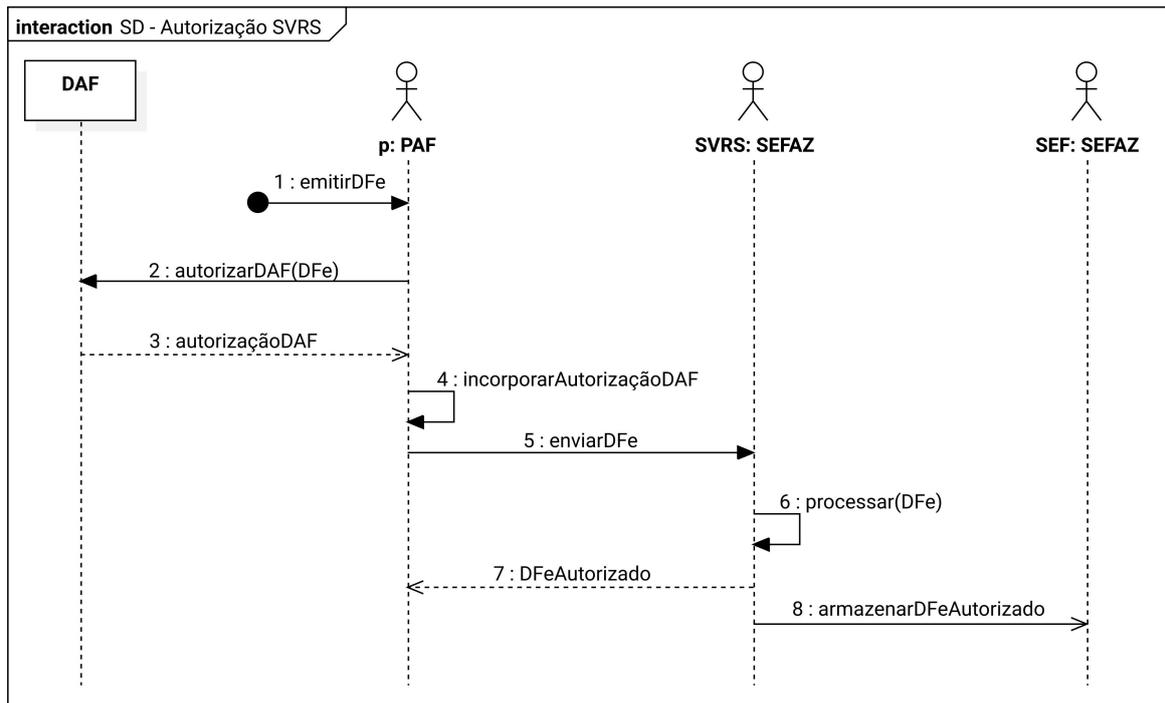
7.6.8 Alterar modo de operação do DAF

A alteração do [modo de operação do DAF](#) fica a critério do contribuinte, que poderá fazê-la sempre que desejado e de acordo com a legislação vigente. O modo de operação indica se o DAF é operado por um único [PDVs](#) ou é compartilhado por mais de um PDV. Todo pedido de alteração do [modo de operação do DAF](#) deverá ser autorizado pela SEF.

7.6.9 Obter resultado sobre autorização de DF-e

De acordo com a decisão do Grupo Especialista Setorial em Automação Comercial da SEF (GESAC), o projeto DAF será usado somente pelo estado de Santa Catarina e a validação da autorização emitida pelo DAF, incluída dentro do XML do DF-e, será validada exclusivamente pela Secretaria de Estado da Fazenda de Santa Catarina (SEF). Sendo assim, dentro do escopo desse projeto, os DF-e seguirão o procedimento de autorização da forma que está descrito em ENCAT (2019a,b) e, dentro do fluxo principal, serão encaminhados para a SEFAZ autorizadora.

Figura 7.2: Diagrama de sequência do processo de autorização de um DF-e



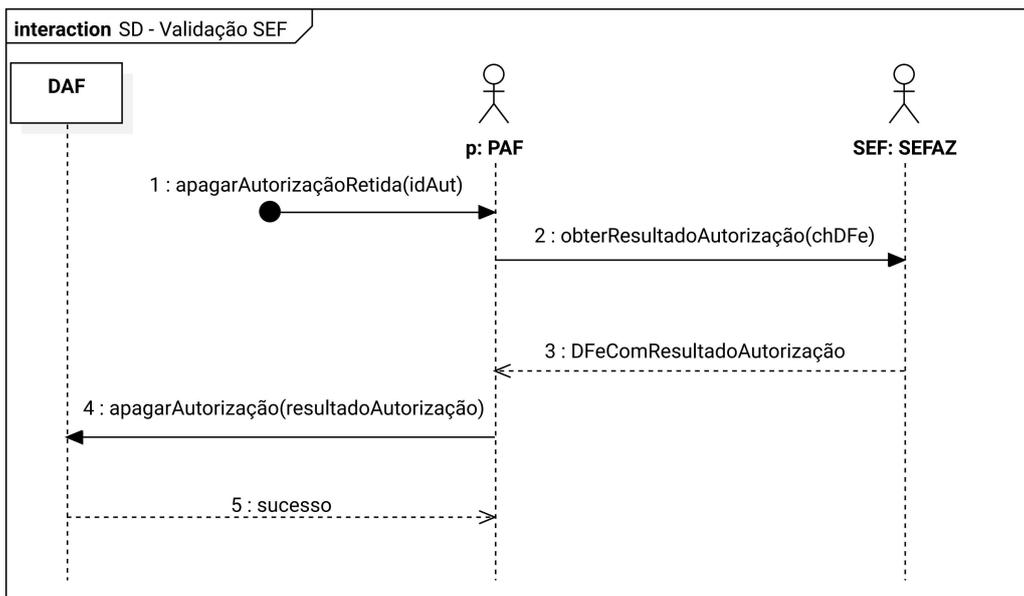
Na Figura 7.2 é ilustrado um diagrama de sequência com o fluxo principal do processo para autorização de DF-e. A SVRS, ao receber o pedido (passo 5) e constatar que o DF-e está correto, então SVRS encaminha ao contribuinte a informação que o DF-e foi autorizado para uso (passo 7). Por meio do serviço de distribuição da SVRS (passo 8), a SEF receberá o documento para que faça a validação do fragmento DAF. O contribuinte, em um momento posterior, precisará interagir com a SEF para obter a autorização que permita ao DAF excluir a autorização retida em sua MT.

Na Figura 7.3 é ilustrado um diagrama de sequência com o fluxo principal do processo de validação de uma autorização emitida pelo DAF. O PAF deve enviar à SEF informações sobre a autorização de um DF-e que fora emitida pelo DAF (passo 2). A SEF verifica se possui o DF-e em sua base e confronta as informações geradas pelo DAF com àquelas que possui em sua base (valor do contador monotônico, assinatura gerada pelo DAF, etc). Se as informações estiverem corretas, atualiza o valor do contador monotônico para aquele DAF e gera uma autorização assinada (passo 3). O PAF encaminha a autorização ao DAF para que esse possa removê-la de sua MT.

7.6.10 Solicitar resultado sobre autorização de DF-e com rejeição

A autorização emitida pelo DAF será validada pela Secretaria de Estado da Fazenda de Santa Catarina (SEF), como descrito na Subseção 7.6.9, por meio do XML de distribuição fornecido pela

Figura 7.3: Diagrama de sequência do processo de validação de autorização gerada pelo DAF



SEFAZ, gerado apenas para DF-e autorizados para uso ou denegados. Deste modo, caso existam autorizações emitidas pelo DAF sobre documentos que resultaram em rejeições, o contribuinte deverá solicitar a validação destas autorizações por meio de um serviço específico da SEF.

Cabe ao PAF manter o XML de todos os DF-e rejeitados, bem como os respectivos protocolos de recebimento enviados pela SEFAZ autorizadora, até que exclua as respectivas autorizações retidas no DAF que comanda. Para solicitar a exclusão dessas autorizações retidas na **MT** o contribuinte deverá encaminhar, juntamente com a chave de acesso do DF-e, os documentos XML enviados a SEFAZ autorizadora e seus respectivos protocolos de recebimento que apresentam os motivos das rejeições (veja [Subseção 8.8.1](#)).

Este serviço permite a consulta de apenas um DF-e por solicitação e cada solicitação poderá conter até 20 versões rejeitadas de um mesmo DF-e, as quais deverão ser ordenadas cronologicamente. Caso um **DF-e** tenha mais de 20 versões rejeitadas, então o PAF deverá invocar esse serviço de forma recorrente até que todas versões sejam encaminhadas à SEF.

7.6.11 Solicitar remoção extraordinária de autorização retida

Toda autorização emitida pelo DAF fica retida em sua **Memória de Trabalho (MT)** e só poderá ser excluída se receber uma autorização gerada pela SEF, como apresentado na [Subseção 7.6.9](#) e [Subseção 7.6.10](#).

Contudo, é possível que aconteçam situações não previstas de forma que uma autorização retida na **MT** não tenha os elementos necessários para que possa ser removida, seguindo os procedimentos descritos na [Subseção 7.6.9](#) ou [Subseção 7.6.10](#). Neste caso, o **contribuinte** poderá recorrer ao serviço da SEF para solicitar a remoção extraordinária de autorização retida (veja [Subseção 8.8.2](#)). Este serviço permite que sejam encaminhadas até 20 autorizações de **DF-e** por solicitação, as quais deverão ordenadas cronologicamente antes do envio. No pedido, o PAF do contribuinte deverá encaminhar a justificativa pra tal solicitação, bem como o **idAut**, o fragmento XML com as informações essenciais do **DF-e** e o **resumo criptográfico** sobre o XML completo do DF-e em questão.

8 Interfaces dos Serviços Web

Neste capítulo são apresentadas as definições das interfaces dos Serviços Web disponibilizadas pela SEF, bem como os critérios técnicos para o consumo dos mesmos pelo PAF do contribuinte. Na Tabela 8.1 é apresentada a relação de Serviços Web providos.

Tabela 8.1: Relação dos Serviços Web providos pela SEF para o PAF do contribuinte

Nome do Serviço Web	Processo	Nome do método	Função
DAFRegistroDispositivo	Síncrono	<code>iniciarRegistro</code>	Recepção de solicitações para iniciar registro do DAF
		<code>confirmarRegistro</code>	Resultado da solicitação de registro do DAF
DAFRemocaoRegistro	Síncrono	<code>removerRegistro</code>	Recepção de solicitações para remover registro do DAF
		<code>confirmarRemoverRegistro</code>	Resultado da remoção de registro DAF
DAFResultadoAutorizacao	Síncrono	<code>obterResultadoAutorizacao</code>	Resultado da validação da autorização do DAF
DAFAutorizacaoRetida	Assíncrono	<code>encaminharDFeRejeitado</code>	Recepção de DF-e rejeitado para validar a autorização do DAF
		<code>encaminharAutorizacoesRetidas</code>	Recepção de solicitação extraordinária para apagar autorizações retidas
		<code>consultarAutorizacaoApagar</code>	Resultado da validação da autorização do DAF de DF-e rejeitado ou de autorização extraordinária para apagar autorização retida no DAF
DAFAvisoExtravio	Síncrono	<code>avisarExtravio</code>	Recepção de notificação de sinistro ocorrido com o DAF
DAFAlteracaoModoOperacao	Síncrono	<code>alterarModoOperacao</code>	Recepção de solicitações para alteração do modo de operação do DAF
		<code>confirmarModoOperacao</code>	Resultado da alteração do modo de operação do DAF
DAFConsultaSB	Síncrono	<code>consultarVersaoSB</code>	Informações sobre a versão atual do SB para um modelo de DAF
DAFAtualizacaoCertificado	Síncrono	<code>solicitarCertificado</code>	Recepção de solicitações de atualização de certificado digital

DAFConsultaDispositivo	Síncrono	consultarDispositivo	Consulta da situação do DAF junto à SEF
DAFSolicitacaoChavePAF	Síncrono	solicitarChavePAF	Recepção das solicitações para recuperação da chave PAF

8.1 Padrões técnicos

8.1.1 Padrão de comunicação

1. A comunicação entre o [PAF](#) e a [SEF](#) será baseada em *Serviços Web* síncronos disponibilizados pela [SEF](#).
 - 1.1. Para os processos síncronos, o envio da solicitação e a obtenção do retorno serão realizados na mesma conexão por meio de um único método do *Serviço Web*;
 - 1.2. Para os processos assíncronos
 - 1.2.1. O método consumido para o envio da solicitação retorna, na mesma conexão, uma mensagem de confirmação de recebimento juntamente com o número do recibo ou retorna uma mensagem de erro;
 - 1.2.2. O método consumido para obter o resultado da solicitação retorna, na mesma conexão, o resultado do processo ou uma mensagem de erro.
2. O meio de comunicação será a Internet, com uso do protocolo [TLS](#) com versão igual ou superior ao utilizado no [ENCAT \(2019a\)](#);
3. O modelo de comunicação segue o padrão de *Serviços Web* definido pelo *Web Services Interoperability Basic Profile (WS-I BP)*. O processo de utilização dos *Serviços Web* sempre é iniciado pela aplicação do contribuinte e a troca de mensagens é realizada no padrão [SOAP](#) versão 1.2 ([W3C, 2007](#)), com mensagens [XML](#) no padrão *Style/Encoding: Document/Literal*.
 - 3.1. A chamada de serviços é iniciada pelo [PAF](#) do [contribuinte](#) e é realizada com o envio de uma mensagem por meio do campo contendo o nome do método a ser invocado. A [Listagem 8.1](#) contém o exemplo de uma mensagem de requisição padrão [SOAP](#);
 - 3.2. A resposta do processamento da requisição pela aplicação da [SEF](#) será realizada com o envio de uma mensagem por meio do campo contendo o nome do método invocado concatenado com a palavra *Response*. A [Listagem 8.2](#) contém o exemplo de uma mensagem de retorno padrão [SOAP](#);
 - 3.3. A ocorrência de qualquer erro na validação dos dados recebidos interrompe o processo com a disponibilização de uma mensagem contendo o código e a descrição do erro conforme a [Seção 8.4](#).

Listagem 8.1: Exemplo de mensagem de requisição SOAP

```

1 <?xml version="1.0" encoding="utf-8"?>
2 <soap12:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.
   org/2001/XMLSchema" xmlns:soap12="http://www.w3.org/2003/05/soap-envelope">
3 <soap12:Body>
4 <iniciarRegistro xmlns="http://www.portalfiscal.inf.br/daf/wsd1/DAFRegistroDispositivo">
```

```

5 <!-- Conteúdo do pedido -->
6 </iniciarRegistro>
7 </soap12:Body>
8 </soap12:Envelope>

```

Listagem 8.2: Exemplo de mensagem de retorno SOAP

```

1 <?xml version="1.0" encoding="utf-8"?>
2 <soap12:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.
   org/2001/XMLSchema" xmlns:soap12="http://www.w3.org/2003/05/soap-envelope">
3 <soap12:Body>
4 <iniciarRegistroResponse xmlns="http://www.portalfiscal.inf.br/daf/wsd/DAFRegistroDispositivo">
5 <!-- Conteúdo da resposta -->
6 </iniciarRegistroResponse>
7 </soap12:Body>
8 </soap12:Envelope>

```

8.1.2 Padrão de assinatura digital

1. As mensagens enviadas à SEF são documentos eletrônicos XML e devem ser assinados digitalmente com um certificado digital emitido por uma **Autoridade Certificadora (AC)** credenciada pela **ICP-Brasil**. Esse certificado deve conter o **CNPJ** do contribuinte detentor do **DAF**.
2. A assinatura do contribuinte será feita no elemento referente ao grupo de informações do pedido que contém o atributo **Id**. O conteúdo do identificador único **Id** deverá ser o **IdDAF** representado em **Base64URL**, precedida do literal **DAF**.
3. O identificador único precedido pela literal ‘#’ deverá ser informado no atributo **URI** do elemento **Reference** da assinatura digital.
4. O leiaute da assinatura digital usada nas mensagens seguem o padrão especificado em **ENCAT (2019a)**. A **Listagem 8.3** contém o exemplo de uma mensagem de entrada assinada.
5. Os procedimentos para validação da assinatura digital seguem os adotados no **ENCAT (2019a)**.

Listagem 8.3: Exemplo de assinatura da mensagem de entrada

```

1 <iniciarRegistro xmlns="http://www.portalfiscal.inf.br/daf/wsd/DAFRegistroDispositivo">
2 <pedRegistro xmlns="http://www.portalfiscal.inf.br/daf" versao="1.00">
3 <infRegistro Id="ughyrcDYBW0zaIGJG3Z6iw">
4 <!-- Conteúdo do pedido -->
5 </infRegistro>
6 <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
7 <SignedInfo>
8 <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
9 <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
10 <Reference URI="#ughyrcDYBW0zaIGJG3Z6iw">
11 <Transforms>
12 <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
13 <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
14 </Transforms>
15 <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
16 <DigestValue>dQXTK2bjTzPLEWKGztY8wuv7f20=</DigestValue>

```

```

17     </Reference>
18   </SignedInfo>
19   <SignatureValue>vhqZ3zpWq580PRyYJdGsKw7JX+oEwYW2wPRpAIgobsC...</SignatureValue>
20   <KeyInfo>
21     <X509Data>
22       <X509Certificate>MIIDjzCCAnegAwIBAgIEF2/aITANBgkqhkiG9w...</X509Certificate>
23     </X509Data>
24   </KeyInfo>
25 </Signature>
26 </pedRegistro>
27 </iniciarRegistro>

```

8.2 Padrão de mensagens XML

1. A especificação do documento XML adotada será a recomendação da W3C para XML 1.0, disponível em Bray et al. (2008), e os caracteres deverão ser codificados em UTF-8;
2. Para serviços correspondentes ao DAF não é permitida a utilização de prefixos de *namespace*. Além disso, a declaração do *namespace* da assinatura digital deverá ser realizada no próprio grupo XML Signature.

Na Tabela 8.2 são apresentadas os nomes das colunas, bem como suas descrições, das tabelas com as definições de leiaute XML que estão presentes neste capítulo.

Tabela 8.2: Cabeçalho das tabelas com definições de leiaute XML

Coluna	Descrição	Valores possíveis
#	código de identificação do campo	
Campo	nome do campo	
Elemento	indica qual é a categoria do campo	A para atributo do elemento pai E para elemento G para elemento de grupo ID para identificador único do elemento pai Raiz para elemento raiz
Pai	indica qual é o elemento pai do campo	
Tipo	indica o tipo do campo	N numérico C alfanumérico D data B lógico XML documento XML
Ocorr.	a-b, sendo (a) para ocorrência mínima e (b) a ocorrência máxima do campo	
Tamanho	x-y, sendo (x) para o tamanho mínimo e (y) para o tamanho máximo do campo. A existência de apenas um único valor indica campo com tamanho fixo	
Descrição	descrição literal do campo	

8.3 Representação de tokens JWT

1. No cabeçalho (*header*) do *token* JWT (JONES; BRADLEY; SAKIMURA, 2015) DEVEM constar somente as chaves `typ` e `alg`, com seus respectivos valores;
 - 1.1. Quando for necessário indicar explicitamente a *chave pública*, par da *chave privada* que foi usada para assinar o *token*, essa será representada dentro do cabeçalho do `jwt` e de acordo com a especificação *JWK* (JONES, 2015b) e *JWA* (JONES, 2018);
 - 1.2. O documento JSON do cabeçalho (*header*) do *token* JWT DEVE ser gerado de forma minimizada, sem espaços em branco ou quebras de linha entre as chaves e os valores do documento.
2. No conteúdo (*payload*) do *token* JWT os nomes dos parâmetros e seus valores DEVEM ser representados como pares chave e valor e DEVEM estar na mesma ordem dentro do documento JSON conforme apresentado nas seções neste capítulo que descrevem os métodos dos *Serviços Web*;
 - 2.1. O documento JSON do conteúdo (*payload*) do *token* JWT DEVE ser gerado de forma minimizada, sem espaços em branco ou quebras de linha entre as chaves e os valores do documento.

8.4 Regras de validação dos Serviços Web

8.4.1 Regras gerais de validação

Serão aplicadas, em todos os *Serviços Web*, as regras gerais de validação dos grupos da [Tabela 8.3](#) as quais estão detalhadas no Anexo II do documento [ENCAT \(2019a\)](#).

Tabela 8.3: Regras gerais de validação

Grupo	Descrição
A	Validação do Certificado de Transmissão (Protocolo TLS)
B	Validação Inicial da Mensagem no Serviço Web
D	Validação da Área de Dados
E	Validação do Certificado Digital de Assinatura
F	Validação de Assinatura Digital

8.4.2 Regras específicas de negócio

Na [Tabela 8.4](#) são apresentados os códigos de resultado de processamento das requisições específicas do [DAF](#).

Tabela 8.4: Tabela de códigos de resultado de processamento

Código	Resultado do processamento da solicitação
1000	Solicitação recebida com sucesso
1001	Dispositivo registrado com sucesso

1002	Registro de dispositivo removido
1003	Consulta de Software Básico efetuada com sucesso
1004	Notificação de extravio efetuada com sucesso
1005	Validação do fragmento DAF realizada com sucesso
1006	Modo de operação alterado com sucesso

Na [Tabela 8.5](#) são apresentados os códigos de erros e descrições das mensagens específicas do DAF.

Tabela 8.5: Tabela de códigos de rejeição de caso de uso

Código	Motivo de não atendimento da solicitação
2000	Rejeição: registro do IdDAF não encontrado
2001	Rejeição: IdPAF não corresponde ao registro do DAF
2002	Rejeição: <i>nonce</i> não corresponde ao informado pela SEF
2003	Rejeição: valor do contador monotônico inválido
2004	Rejeição: assinatura de <i>token</i> inválida
2005	Rejeição: CNPJ do contribuinte registrado diverge do CNPJ da assinatura
2006	Rejeição: IdPAF não registrado
2007	Rejeição: DAF extraviado
2008	Rejeição: IdDAF do <i>token</i> não corresponde ao IdDAF informado
2009	Rejeição: DAF em situação irregular
2010	Rejeição: justificativa inválida. A justificativa deve conter entre 15 e 255 caracteres
2011	Rejeição: consumo indevido pelo aplicativo da empresa. Permitido no máximo 40 requisições por hora
2012	Rejeição: CNPJ do fabricante DAF inválido
2013	Rejeição: modelo DAF inválido
2100	Rejeição: <i>hash</i> do IdPAF diverge do calculado
2101	Rejeição: assinatura gerada pela chave de ateste não corresponde a um modelo de DAF certificado
2102	Rejeição: CNPJ do responsável técnico inválido
2103	Rejeição: identificador do CSRT (tag:idCSRT) não cadastrado na SEF
2104	Rejeição: identificador do CSRT (tag:idCSRT) revogado
2105	Rejeição: CNPJ do contribuinte não cadastrado
2108	Rejeição: CNPJ do responsável técnico não cadastrado
2300	Rejeição: IdDAF do requerente não corresponde ao IdDAF de autorização do DF-e
2301	Rejeição: chave DF-e não encontrada
2302	Rejeição: DAF deve atualizar a versão do software básico
2303	Rejeição: versão do software básico do DAF está desatualizada
2304	Rejeição: <i>token</i> de autorização inválido
2400	Rejeição: remoção extraordinária de autorização retida indisponível para o contribuinte
2401	Rejeição: número de recibo não encontrado
2402	Rejeição: lote em processamento
2403	Rejeição: a rejeição informada para o DF-e é inválida
2404	Rejeição: as informações essenciais do DF-e são inválidas
2500	Rejeição: notificação de extravio do DAF já foi realizada
2600	Rejeição: o modo de operação já informado anteriormente

8.5 Serviço *Web* - DAFRegistroDispositivo

Este serviço, composto pelos métodos `iniciarRegistro` e `confirmarRegistro`, permite ao PAF do contribuinte registrar seu DAF junto à SEF. Trata-se de um processo síncrono. O processo operacional detalhado está descrito na [Subseção 7.6.1](#).

8.5.1 `iniciarRegistro`

Função: atender solicitações para iniciar o processo de registro de DAF.

8.5.1.1 Leiaute mensagem de entrada

Entrada: estrutura XML contendo a solicitação de registro do DAF (veja [Tabela 8.6](#)).

Tabela 8.6: Leiaute da mensagem de entrada do método `iniciarRegistro`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PRD01	<code>pedRegistro</code>	Raiz	-	-	-	-	TAG raiz
PRD02	<code>versao</code>	A	PRD01	C	1-1	4	versão do leiaute
PRD03	<code>infRegistro</code>	G	PRD01	-	1-1	-	grupo de informações necessárias para o registro do DAF
PRD04	<code>Id</code>	ID	PRD03	C	1-1	25	identificador da TAG a ser assinada. Deve-se informar o <code>IdDAF</code> , representado em Base64URL, precedida do literal <code>DAF</code>
PRD05	<code>IdDAF</code>	E	PRD03	C	1-1	22	Identificador único do DAF representado em Base64URL
PRD06	<code>IdPAF</code>	E	PRD03	C	1-1	43	Identificador único do PAF
PRD07	<code>modeloDaf</code>	E	PRD03	C	1-1	1-20	Nome do modelo DAF
PRD08	<code>cnpjFabricante</code>	E	PRD03	C	1-1	14	CNPJ do fabricante DAF
PRD09	<code>cnpjContribuinte</code>	E	PRD03	C	1-1	14	CNPJ do contribuinte
PRD10	<code>cnpjResponsavel</code>	E	PRD03	C	1-1	14	CNPJ do responsável técnico
PRD11	<code>idCSRT</code>	E	PRD03	N	1-1	1	identificador do CSRT
PRD12	<code>modoOp</code>	E	PRD03	B	1-1	1	modo de operação do DAF. Preencher com <code>false</code> em caso de DAF não compartilhado, um DAF por PDV; ou com <code>true</code> em caso de DAF compartilhado por mais de um PDV
PRD14	<code>Signature</code>	G	PRD01	XML	1-1	-	assinatura XML do grupo identificado pelo atributo <code>Id</code>

8.5.1.2 Leiaute mensagem de retorno

Retorno: estrutura XML contendo a mensagem de retorno da solicitação de registro do DAF (veja [Tabela 8.7](#)).

Tabela 8.7: Leiaute da mensagem de retorno do método `iniciarRegistro`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
RRD01	<code>retRegistro</code>	Raiz	-	-	-	-	TAG raiz
RRD02	<code>versao</code>	A	RRD01	C	1-1	4	versão do leiaute
RRD03	<code>IdDAF</code>	E	RRD01	C	1-1	22	Identificador único do DAF representado em Base64URL
RRD04	<code>cStat</code>	E	RRD01	N	1-1	3-4	código de <i>status</i> da resposta (veja Tabela 8.9)
RRD05	<code>xMotivo</code>	E	RRD01	C	1-1	1-255	descrição literal do <i>status</i> da resposta
RRD06	<code>tkDesafio</code>	E	RRD01	C	0-1	300-500	<i>token JWT</i> contendo o desafio gerado pela SEF (veja Tabela 8.8)

O campo RRD06, indicado na [Tabela 8.7](#), tem por objetivo conter um *token JWT* (veja [Seção 8.3](#)), cujo conteúdo (*payload*) está descrito na [Tabela 8.8](#).

Tabela 8.8: Conteúdo do `tkDesafio` da mensagem de retorno do `iniciarRegistro`

Nome do parâmetro	Tamanho (bytes)	Tipo	Descrição
<code>nnc</code>	22	<i>string</i>	valor aleatório gerado pela SEF representado em Base64URL

8.5.1.3 Validações

Na [Tabela 8.9](#) são apresentados os códigos de rejeição que poderão ser retornados após a aplicação das validações das regras de negócio.

Tabela 8.9: Códigos de rejeição da mensagem de entrada do método `iniciarRegistro`

Código	Descrição
2005	CNPJ do contribuinte diverge do CNPJ da assinatura
2011	consumo indevido pelo aplicativo da empresa. Permitido no máximo 40 requisições por hora
2012	CNPJ do fabricante DAF inválido
2013	modelo DAF inválido
2100	<i>hash</i> do <code>IdPAF</code> diverge do calculado
2102	CNPJ do responsável técnico inválido
2103	identificador do CSRT (tag: <code>idCSRT</code>) não cadastrado na SEF
2104	identificador do CSRT (tag: <code>idCSRT</code>) revogado
2105	CNPJ do contribuinte não cadastrado

8.5.1.4 Final do processamento

Em caso de sucesso o processamento do pedido para iniciar o registro do DAF retorna um *nonce* gerado pela SEF e o `cStat` com o valor 1000 da [Tabela 8.4](#). Caso contrário resulta em uma mensagem de erro conforme [Tabela 8.9](#).

8.5.2 confirmarRegistro

Função: efetivar o registro do DAF junto à SEF.

8.5.2.1 Leiaute mensagem de entrada

Entrada: estrutura XML da mensagem para confirmar o registro do DAF (veja Tabela 8.10).

Tabela 8.10: Leiaute da mensagem de entrada do método `confirmarRegistro`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PCD01	<code>pedConfRegistro</code>	Raiz	-	-	-	-	TAG raiz
PCD02	<code>versao</code>	A	PCD01	C	1-1	4	versão do leiaute
PCD03	<code>infConfRegistro</code>	G	PCD01	-	1-1	-	informações para a confirmação do registro
PCD04	<code>Id</code>	ID	PCD03	C	1-1	25	identificador da TAG a ser assinada. Deve-se informar o <code>IdDAF</code> , representado em Base64URL, precedida do literal <code>DAF</code>
PCD06	<code>IdDAF</code>	E	PCD03	C	1-1	22	Identificador único do DAF representado em Base64URL
PCD07	<code>IdPAF</code>	E	PCD03	C	1-1	43	Identificador único do PAF
PCD05	<code>tkAut</code>	E	PCD03	C	1-1	2.900-3.100	<i>token</i> JWT com informações para registro (veja Tabela 8.11)
PCD08	<code>Signature</code>	G	PCD01	XML	1-1	-	assinatura XML do grupo identificado pelo atributo <code>Id</code>

O campo PCD05, indicado na Tabela 8.10, tem por objetivo conter um *token* JWT (veja Seção 8.3) que fora assinado com a *chave de ateste* do DAF, cuja *chave pública* correspondente deverá estar de forma explícita no cabeçalho do *token* e terá como conteúdo (*payload*) uma chave `jwt`. O valor associado a essa chave `jwt` será outro *token* JWT, o qual foi assinado com a *chave privada* do DAF, cuja *chave pública* correspondente deverá estar de forma explícita no cabeçalho do *token* e ter como conteúdo as informações apresentadas na Tabela 8.11.

Tabela 8.11: Conteúdo do `tkAut` da mensagem de entrada do método `confirmarRegistro`

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
<code>daf</code>	22	<i>string</i>	<code>IdDAF</code> representado em Base64URL
<code>cnt</code>	4	inteiro	valor atual do contador monotônico
<code>nnc</code>	22	<i>string</i>	valor aleatório gerado pela SEF representado em Base64URL

8.5.2.2 Leiaute mensagem de retorno

Retorno: estrutura XML da mensagem de retorno da efetivação do registro do DAF (veja Tabela 8.12).

Tabela 8.12: Leiaute da mensagem de retorno do método `confirmarRegistro`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
RCD01	<code>retConfRegistro</code>	Raiz	-	-	-	-	TAG raiz
RCD02	<code>versao</code>	A	RCD01	C	1-1	4	versão do leiaute
RCD03	<code>IdDAF</code>	E	RCD01	C	1-1	22	Identificador único do DAF representado em Base64URL

RCD04	cStat	E	RCD01	N	1-1	3-4	código de <i>status</i> da resposta (veja Tabela 8.14)
RCD05	xMotivo	E	RCD01	C	1-1	1-255	descrição literal do status da resposta
RCD06	tkChaves	E	RCD01	C	0-1	850-1.050	JWT contendo as informações de retorno do registro (veja Tabela 8.13)

O campo RCD06, indicado na [Tabela 8.12](#), tem por objetivo conter um *token JWT* (veja [Seção 8.3](#)), cujo conteúdo (*payload*) está descrito na [Tabela 8.13](#).

Tabela 8.13: Conteúdo do tkChaves da mensagem de retorno do confirmarRegistro

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
chs	variável	<i>string</i>	Chave SEF cifrada com a chave pública do DAF, com o esquema de cifragem RSAES-OAEP (MORIARTY et al., 2016) ou ECIES (ANSI, 2001), e representada em Base64URL
chp	86	<i>string</i>	Chave PAF representada em Base64URL
mop	1	inteiro	modo de operação do DAF. 0 = DAF não compartilhado, um DAF por PDV; 1 = DAF compartilhado por mais de um PDV

8.5.2.3 Validações

Na [Tabela 8.14](#) são apresentados os códigos de rejeição que poderão ser retornados após a aplicação das validações das regras de negócio.

Tabela 8.14: Códigos de rejeição da mensagem de entrada do método confirmarRegistro

Código	Descrição
2000	registro do IdDAF não encontrado
2001	IdPAF não corresponde ao registro do DAF
2002	<i>nonce</i> não corresponde ao informado pela SEF
2003	valor do contador monotônico inválido
2004	assinatura de <i>token</i> inválida
2005	CNPJ do contribuinte diverge do CNPJ da assinatura
2006	IdPAF não registrado
2008	IdDAF do <i>token</i> não corresponde ao IdDAF informado
2009	DAF em situação irregular
2011	consumo indevido pelo aplicativo da empresa. Permitido no máximo 40 requisições por hora
2013	modelo DAF inválido
2101	assinatura gerada pela chave de ateste não corresponde a um modelo de DAF certificado

8.5.2.4 Final do processamento

Em caso de sucesso o processamento do pedido de confirmação do registro do **DAF** retorna as chaves criptográficas geradas pela **SEF** e o cStat com o valor 1001 da [Tabela 8.4](#). Caso contrário, resulta em uma mensagem de erro conforme [Tabela 8.14](#).

8.6 Serviço Web - DAFRemocaoRegistro

Serviço destinado a remover as informações de registro do DAF junto à SEF. O serviço é composto pelos métodos `removerRegistro` e `confirmarRemoverRegistro`. Trata-se de um processo síncrono. O processo operacional detalhado está descrito na Subseção 7.6.2.

8.6.1 `removerRegistro`

Função: atender solicitações para remover informações de registro do DAF junto à SEF.

8.6.1.1 Leiaute mensagem de entrada

Entrada: estrutura XML da mensagem para solicitar remoção do registro do DAF (veja Tabela 8.15).

Tabela 8.15: Leiaute da mensagem de entrada do método `removerRegistro`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PRR01	<code>pedRemRegistro</code>	Raiz	-	-	-	-	TAG raiz
PRR02	<code>versao</code>	A	PRR01	C	1-1	4	versão do leiaute
PRR03	<code>infRemRegistro</code>	G	PRR01	-	1-1	-	informações para a solicitação de remoção do registro
PRR04	<code>Id</code>	ID	PRR03	C	1-1	25	identificador da TAG a ser assinada. Deve-se informar o <code>IdDAF</code> , representado em Base64URL, precedida do literal <code>DAF</code>
PRR05	<code>IdDAF</code>	E	PRR03	C	1-1	22	Identificador único do DAF representado em Base64URL
PRR06	<code>IdPAF</code>	E	PRR03	C	1-1	43	Identificador único do PAF
PRR07	<code>xJust</code>	E	PRR03	C	1-1	15-255	justificativa da remoção de registro
PRR08	<code>Signature</code>	G	PRR01	XML	1-1	-	assinatura XML do grupo identificado pelo atributo <code>Id</code>

8.6.1.2 Leiaute mensagem de retorno

Retorno: estrutura XML da mensagem de retorno da solicitação de remoção do registro do DAF (veja Tabela 8.16).

Tabela 8.16: Leiaute da mensagem de retorno do método `removerRegistro`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
RRR01	<code>retRemRegistro</code>	Raiz	-	-	-	-	TAG raiz
RRR02	<code>versao</code>	A	RRR01	C	1-1	4	versão do leiaute
RRR03	<code>IdDAF</code>	E	RRR01	C	1-1	22	Identificador único do DAF representado em Base64URL
RRR04	<code>cStat</code>	E	RRR01	N	1-1	3-4	código de <i>status</i> da resposta (veja Tabela 8.18)
RRR05	<code>xMotivo</code>	E	RRR01	C	1-1	1-255	descrição literal do <i>status</i> da resposta
RRR06	<code>tkDesafio</code>	E	RRR01	C	0-1	300-500	<i>token</i> JWT (veja Tabela 8.16)

O campo RRR06, indicado na [Tabela 8.16](#), tem por objetivo conter um *token JWT* (veja [Seção 8.3](#)), cujo conteúdo (*payload*) está descrito na [Tabela 8.17](#).

Tabela 8.17: Conteúdo do tkDesafio da mensagem de retorno do `removeRegistro`

Nome do parâmetro	Tamanho (<i>bytes</i>)	Tipo	Descrição
nnc	22	string	valor aleatório gerado pela SEF representado em Base64URL

8.6.1.3 Validações

Na [Tabela 8.18](#) são apresentados os códigos de rejeição que poderão ser retornados após a aplicação das validações das regras de negócio.

Tabela 8.18: Códigos de rejeição da mensagem de entrada do método `removeRegistro`

Código	Descrição
2000	registro do IdDAF não encontrado
2001	IdPAF não corresponde ao registro do DAF
2005	CNPJ do contribuinte diverge do CNPJ da assinatura
2007	DAF extraviado
2009	DAF em situação irregular
2010	justificativa inválida. A justificativa deve conter entre 15 e 255 caracteres
2011	consumo indevido pelo aplicativo da empresa. Permitido no máximo 40 requisições por hora

8.6.1.4 Final do processamento

Em caso de sucesso o processamento do pedido para remover o registro do **DAF** retorna um *nonce* gerado pela SEF e o `cStat` com o valor 1000 da [Tabela 8.4](#). Caso contrário resulta em uma mensagem de erro conforme [Tabela 8.18](#).

8.6.2 confirmarRemoveRegistro

Função: confirmar a remoção das informações de registro do **DAF** junto à SEF.

8.6.2.1 Leiaute mensagem de entrada

Entrada: estrutura **XML** da mensagem para remoção do registro do **DAF** (veja [Tabela 8.19](#)).

Tabela 8.19: Leiaute da mensagem de entrada do método `confirmarRemoveRegistro`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PCR01	pedConfRemRegistro	Raiz	-	-	-	-	TAG raiz
PCR02	versao	A	PCR01	C	1-1	4	versão do leiaute
PCR03	infConfRemRegistro	G	PCR01	-	1-1	-	informações para a confirmação de remoção do registro

PCR04	Id	ID	PCR03	C	1-1	25	identificador da TAG a ser assinada. Deve-se informar o IdDAF, representado em Base64URL, precedida do literal <i>DAF</i>
PCR05	IdDAF	E	PCR03	C	1-1	22	Identificador único do DAF representado em Base64URL
PCR06	IdPAF	E	PCR03	C	1-1	43	Identificador único do PAF
PCR07	tkAut	E	PCR03	C	1-1	400-600	token JWT (veja Tabela 8.20)
PCR08	Signature	G	PCR01	XML	1-1	-	assinatura XML do grupo identificado pelo atributo Id

O campo PCR07, indicado na Tabela 8.19, tem por objetivo conter um *token JWT* (veja Seção 8.3), cujo conteúdo (*payload*) está descrito na Tabela 8.20.

Tabela 8.20: Conteúdo do tkAut da mensagem de entrada do confirmarRemoveRegistro

Nome do parâmetro	Tamanho (bytes)	Tipo	Descrição
daf	22	string	Identificador único do DAF representado em Base64URL
cnt	4	inteiro	valor atual do contador monotônico
mnc	22	string	valor aleatório gerado pela SEF representado em Base64URL

8.6.2.2 Leiaute mensagem de retorno

Retorno: estrutura XML da mensagem de retorno de confirmação de remoção do registro do DAF (veja Tabela 8.21).

Tabela 8.21: Leiaute da mensagem de retorno do método confirmarRemoveRegistro

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
RCR01	retConfRemRegistro	Raiz	-	-	-	-	TAG raiz
RCR02	versao	A	RCR01	C	1-1	4	versão do leiaute
RCR03	IdDAF	E	RCR01	C	1-1	22	Identificador único do DAF representado em Base64URL
RCR04	cStat	E	RCR01	N	1-1	3-4	código de <i>status</i> da resposta (veja Tabela 8.23)
RCR05	xMotivo	E	RCR01	C	1-1	1-255	descrição literal do <i>status</i> da resposta
RCR06	tkEvento	E	RCR01	C	0-1	300-500	token JWT (veja Tabela 8.22)

O campo RCR06, indicado na Tabela 8.21, tem por objetivo conter um *token JWT* (veja Seção 8.3), cujo conteúdo (*payload*) está descrito na Tabela 8.22.

Tabela 8.22: Conteúdo do tkEvento da mensagem de retorno do confirmarRemoveRegistro

Nome do parâmetro	Tamanho (bytes)	Tipo	Descrição
evn	7	string	cadeia de caracteres REMOVE

8.6.2.3 Validações

Na [Tabela 8.23](#) são apresentados os códigos de rejeição que poderão ser retornados após a aplicação das validações das regras de negócio.

Tabela 8.23: Códigos de rejeição da mensagem de entrada do método `confirmarRemoverRegistro`

Código	Descrição
2000	registro do IdDAF não encontrado
2001	IdPAF não corresponde ao registro do DAF
2002	<i>nonce</i> não corresponde ao informado pela SEF
2003	valor do contador monotônico inválido
2004	assinatura de <i>token</i> inválida
2005	CNPJ do contribuinte diverge do CNPJ da assinatura
2008	IdDAF do <i>token</i> não corresponde ao IdDAF informado
2009	DAF em situação irregular
2011	consumo indevido pelo aplicativo da empresa. Permitido no máximo 40 requisições por hora

8.6.2.4 Final do processamento

Em caso de sucesso o processamento da confirmação da remoção do registro do [DAF](#) retorna uma instrução de remoção e o `cStat` com o valor 1002 da [Tabela 8.4](#). Caso contrário, resulta em uma mensagem de erro conforme [Tabela 8.23](#).

8.7 Serviço Web - `DAFResultadoAutorizacao`

Permite obter o resultado da validação do fragmento [DAF](#) junto à [SEF](#). O serviço é composto pelo método `obterResultadoAutorizacao`. Trata-se de um processo síncrono. O processo operacional detalhado está descrito na [Subseção 7.6.9](#).

8.7.1 `obterResultadoAutorizacao`

Função: obter o resultado da validação do fragmento [DAF](#).

8.7.1.1 Leiaute mensagem de entrada

Entrada: estrutura [XML](#) da mensagem para a solicitação do resultado do processamento do fragmento [DAF](#) (veja [Tabela 8.24](#)).

Tabela 8.24: Leiaute da mensagem de entrada do método `obterResultadoAutorizacao`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PRA01	<code>pedAutorizacao</code>	Raiz	-	-	-	-	TAG raiz
PRA02	<code>versao</code>	A	PRA01	C	1-1	4	versão do leiaute
PRA03	<code>infAutorizacao</code>	G	PRA01	-	1-1	-	informações para o processamento do fragmento DAF

PRA04	Id	ID	PRA03	C	1-1	25	identificador da TAG a ser assinada. Deve-se informar o IdDAF, representado em Base64URL, precedida do literal <i>DAF</i>
PRA05	IdDAF	E	PRA03	C	1-1	22	Identificador único do DAF representado em Base64URL
PRA06	IdPAF	E	PRA03	C	1-1	43	Identificador único do PAF
PRA07	chDFe	E	PRA03	C	1-50	44	chave de acesso do DF-e
PRA08	Signature	G	PRA01	XML	1-1	-	assinatura XML do grupo identificado pelo atributo Id

8.7.1.2 Leiaute mensagem de retorno

Retorno: estrutura XML da mensagem de retorno do resultado do processamento do fragmento DAF (veja Tabela 8.25).

Tabela 8.25: Leiaute da mensagem de retorno do método obterResultadoAutorizacao

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
RRA01	retAutorizacao	Raiz	-	-	1-1	-	informações sobre o processamento do fragmento DAF .
RRA02	versao	A	RRA01	C	1-1	4	versão do leiaute
RRA03	IdDAF	E	RRA01	C	1-1	22	Identificador único do DAF
RRA04	cStat	E	RRA01	N	1-1	3-4	código de <i>status</i> da resposta (veja Tabela 8.27)
RRA05	xMotivo	E	RRA01	C	1-1	1-255	descrição literal do <i>status</i> da resposta
RRA06	retDFe	G	RRA01	C	0-50	-	informações sobre o processamento do fragmento DAF
RRA07	chDFe	E	RRA06	C	1-1	44	chave de acesso do DF-e
RRA08	idAut	E	RRA06	C	0-1	43	identificador único da autorização
RRA09	hAut	E	RRA06	C	0-1	43	saída de uma função HMAC, representada em base64URL, que teve como chave a chave SEFAZ e como mensagem o idAut
RRA10	cStatAut	E	RRA06	N	1-1	3-4	código de <i>status</i> da resposta de autorização (veja Tabela 8.26)
RRA11	xMotAut	E	RRA06	C	1-1	1-255	descrição literal do <i>status</i> da resposta de autorização

8.7.1.3 Validações

Na Tabela 8.26 são apresentados os códigos de rejeição que poderão ser retornados após a validação do processamento do fragmento DAF.

Tabela 8.26: Códigos de rejeição sobre a validação do processamento do fragmento DAF

Código	Descrição
2003	valor do contador monotônico inválido
2004	assinatura de <i>token</i> inválida

2300	IdDAF do requerente não corresponde ao IdDAF de autorização do DF-e
2301	chave DF-e não encontrada
2302	DAF deve atualizar a versão do software básico
2303	versão do software básico do DAF está desatualizada
2304	token de autorização inválido

Na [Tabela 8.27](#) são apresentados os códigos de rejeição que poderão ser retornados após a aplicação das validações das regras de negócio.

Tabela 8.27: Códigos de rejeição da mensagem de entrada do método obterResultadoAutorizacao

Código	Descrição
2001	IdPAF não corresponde ao registro do DAF
2005	CNPJ do contribuinte diverge do CNPJ da assinatura
2006	IdPAF não registrado
2007	DAF extraviado
2009	DAF em situação irregular
2011	consumo indevido pelo aplicativo da empresa. Permitido no máximo 40 requisições por hora
2300	IdDAF do requerente não corresponde ao IdDAF de autorização do DF-e
2301	chave DF-e não encontrada

8.7.1.4 Final do processamento

Em caso de sucesso o processamento da consulta retorna o resultado da validação do fragmento DAF, o cStatAut com o valor 1005 e cStat com o valor 1000 da [Tabela 8.4](#). Caso contrário resulta em uma mensagem de erro conforme a [Tabela 8.26](#) e a [Tabela 8.27](#).

8.8 Serviço Web - DAFAutorizacaoRetida

Esse serviço pode ser consumido para excluir da [Memória de Trabalho \(MT\)](#) do DAF autorizações retidas referentes a DF-e rejeitados no processo de autorização junto à SEFAZ autorizadora ou ainda de autorizações retidas que não tenham os elementos necessários para que possam ser removidas, conforme descrito na [Subseção 7.6.11](#). O serviço é composto por três métodos:

- `encaminharDFeRejeitado`;
- `encaminharAutorizacoesRetidas`;
- `consultarAutorizacaoApagar`.

Por se tratar de um processo assíncrono, o PAF deve aguardar um tempo mínimo entre a requisição aos métodos `encaminharDFeRejeitado` ou `encaminharAutorizacoesRetidas`, e ao método `consultarAutorizacaoApagar`, evitando assim a obtenção desnecessária do código de erro 2402 - "Lote em processamento". A especificação do tempo mínimo está fora do escopo deste documento e tal informação deverá ser consultada na especificação de requisitos do PAF. O processo operacional está descrito na [Subseção 5.2.4](#), [Subseção 7.6.11](#) e [Seção 5.4](#).

Os métodos `encaminharDFeRejeitado` e `consultarAutorizacaoApagar` devem ser usados quando se deseja excluir autorização retida de DF-e rejeitado pela SEFAZ autorizadora. Para a remoção

extraordinária de autorização retida deve-se usar os métodos [encaminharAutorizacoesRetidas](#) e [consultarAutorizacaoApagar](#).

8.8.1 encaminharDFeRejeitado

Função: solicitar a validação do fragmento **DAF** contido em **DF-e** rejeitado pela SEFAZ autorizadora.

8.8.1.1 Leiaute mensagem de entrada

Entrada: estrutura **XML** da mensagem para solicitar permissão para apagar autorizações retidas no **DAF** referentes a **DF-e** com rejeições (veja [Tabela 8.28](#)).

Tabela 8.28: Leiaute da mensagem de entrada do método [encaminharDFeRejeitado](#)

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PEJ01	pedEncRejeitado	Raiz	-	-	-	-	TAG raiz
PEJ02	versao	A	PEJ01	C	1-1	4	versão do leiaute
PEJ03	infEncRejeitado	G	PEJ01	-	1-1	-	informações para a solicitação de permissão para apagar autorizações retidas no DAF referentes a DF-e com rejeições
PEJ04	Id	ID	PEJ03	C	1-1	25	identificador da TAG a ser assinada. Deve-se informar o IdDAF , representado em Base64URL, precedida do literal DAF
PEJ05	IdDAF	E	PEJ03	C	1-1	22	Identificador único do DAF representado em Base64URL
PEJ06	IdPAF	E	PEJ03	C	1-1	43	Identificador único do PAF
PEJ07	chDFe	E	PEJ03	C	1-1	44	chave de acesso do DF-e
PEJ08	rejDFe	G	PEJ03	-	1-20	-	informações sobre o documento rejeitado
PEJ09	DFe	E	PEJ08	XML	1-1	-	XML do DF-e enviado para o serviço de autorização
PEJ10	protDFe	E	PEJ08	XML	1-1	-	XML de resposta do serviço de autorização com a rejeição e assinatura da SEFAZ
PEJ11	Signature	G	PEJ01	XML	1-1	-	assinatura XML do grupo identificado pelo atributo Id

8.8.1.2 Leiaute mensagem de retorno

Retorno: estrutura **XML** da mensagem de retorno da solicitação de permissão para apagar autorizações retidas no **DAF** referentes a **DF-e** rejeitados (veja [Tabela 8.29](#)).

Tabela 8.29: Leiaute da mensagem de retorno do método [encaminharDFeRejeitado](#)

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
REJ01	retEncRejeitado	Raiz	-	-	-	-	TAG raiz
REJ02	versao	A	REJ01	C	1-1	4	versão do leiaute

REJ03	IdDAF	E	REJ01	C	1-1	22	Identificador único do DAF representado em Base64URL
REJ04	cStat	E	REJ01	N	1-1	3-4	código de <i>status</i> da resposta (veja Tabela 8.30)
REJ05	xMotivo	E	REJ01	C	1-1	1-255	descrição literal do <i>status</i> da resposta
REJ06	nRec	E	REJ01	N	0-1	15	número do recibo gerado pela SEF

8.8.1.3 Validações

Na Tabela 8.30 são apresentados os códigos de rejeição que poderão ser retornados após a aplicação das validações das regras de negócio.

Tabela 8.30: Códigos de rejeição da mensagem de entrada do método `encaminharDFeRejeitado`

Código	Descrição
2001	IdPAF não corresponde ao registro do DAF
2005	CNPJ do contribuinte diverge do CNPJ da assinatura
2006	IdPAF não registrado
2007	DAF extraviado
2009	DAF em situação irregular
2011	consumo indevido pelo aplicativo da empresa. Permitido no máximo 40 requisições por hora

8.8.1.4 Final do processamento

Em caso de sucesso o processamento do pedido para solicitação de permissão para apagar autorizações retidas no DAF referentes a DF-e rejeitados o `cStat` com o valor 1000 da Tabela 8.4. Caso contrário resulta em uma mensagem de erro conforme Tabela 8.30.

8.8.2 `encaminharAutorizacoesRetidas`

Função: solicitar a remoção extraordinária de autorização retida na MT do DAF.

8.8.2.1 Leiaute mensagem de entrada

Entrada: estrutura XML da mensagem para solicitar a remoção extraordinária de autorizações retidas no DAF (veja Tabela 8.31).

Tabela 8.31: Leiaute da mensagem de entrada do método `encaminharAutorizacoesRetidas`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PER01	<code>pedEncRetida</code>	Raiz	-	-	-	-	TAG raiz
PER02	<code>versao</code>	A	PER01	C	1-1	4	versão do leiaute
PER03	<code>infEncRetida</code>	G	PER01	-	1-1	-	informações para a solicitação de permissão extraordinária para apagar autorizações retidas no DAF

PER04	Id	ID	PER03	C	1-1	25	identificador da TAG a ser assinada. Deve-se informar o IdDAF, representado em Base64URL, precedida do literal <i>DAF</i>
PER05	IdDAF	E	PER03	C	1-1	22	Identificador único do DAF representado em Base64URL
PER06	IdPAF	E	PER03	C	1-1	43	Identificador único do PAF
PER07	xJust	E	PER03	C	1-1	15-255	descrição do problema que justifica a solicitação extraordinária
PER08	autRetida	G	PER03	-	1-20	-	informações sobre o documento rejeitado
PER09	idAut	E	PER08	C	1-1	43	Identificador único da autorização DAF representado em Base64URL
PER10	fragEssencial	E	PER08	XML	1-1	-	XML com as informações essenciais do DF-e
PER11	resumoDFe	E	PER08	C	1-1	43	Resumo criptográfico do DF-e completo representado em Base64URL
PER12	Signature	G	PER01	XML	1-1	-	assinatura XML do grupo identificado pelo atributo Id

8.8.2.2 Leiaute mensagem de retorno

Retorno: estrutura XML da mensagem de retorno da solicitação de permissão para apagar autorizações retidas no DAF referentes a DF-e rejeitados (veja Tabela 8.32).

Tabela 8.32: Leiaute da mensagem de retorno do método `encaminharAutorizacoesRetidas`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
RER01	retEncRetida	Raiz	-	-	-	-	TAG raiz
RER02	versao	A	RER01	C	1-1	4	versão do leiaute
RER03	IdDAF	E	RER01	C	1-1	22	Identificador único do DAF representado em Base64URL
RER04	cStat	E	RER01	N	1-1	3-4	código de <i>status</i> da resposta (veja Tabela 8.33)
RER05	xMotivo	E	RER01	C	1-1	1-255	descrição literal do <i>status</i> da resposta
RER06	nRec	E	RER01	N	0-1	15	número do recibo gerado pela SEF

8.8.2.3 Validações

Na Tabela 8.33 são apresentados os códigos de rejeição que poderão ser retornados após a aplicação das validações das regras de negócio.

Tabela 8.33: Códigos de rejeição do método `encaminharAutorizacoesRetidas`

Código	Descrição
2001	IdPAF não corresponde ao registro do DAF
2005	CNPJ do contribuinte diverge do CNPJ da assinatura
2006	IdPAF não registrado

2007	DAF extraviado
2009	DAF em situação irregular
2011	consumo indevido pelo aplicativo da empresa. Permitido no máximo 40 requisições por hora

8.8.2.4 Final do processamento

Em caso de sucesso o processamento do pedido para remoção extraordinária de autorizações retidas no DAF o cStat com o valor 1000 da [Tabela 8.4](#). Caso contrário resulta em uma mensagem de erro conforme [Tabela 8.33](#).

8.8.3 consultarAutorizacaoApagar

Função: obter o resultado da validação do fragmento DAF de DF-e rejeitado pela SEFAZ autorizadora, e que foi encaminhado à SEF por meio do método [encaminharDFeRejeitado](#) ou de solicitação para remoção extraordinária de autorizações retidas, que foi encaminhada à SEF por meio do método [encaminharAutorizacoesRetidas](#) deste Serviço Web.

8.8.3.1 Leiaute mensagem de entrada

Entrada: estrutura XML da mensagem para obter permissão para apagar autorizações retidas no DAF (veja [Tabela 8.34](#)).

Tabela 8.34: Leiaute da mensagem de entrada do método consultarAutorizacaoApagar

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PCA01	pedConsAutApagar	Raiz	-	-	-	-	TAG raiz
PCA02	versao	A	PCA01	C	1-1	4	versão do leiaute
PCA03	infConsAutApagar	G	PCA01	-	1-1	-	informações para obter permissão para apagar autorizações retidas no DAF
PCA04	Id	ID	PCA03	C	1-1	25	identificador da TAG a ser assinada. Deve-se informar o IdDAF, representado em Base64URL, precedida do literal DAF
PCA05	IdDAF	E	PCA03	C	1-1	22	Identificador único do DAF representado em Base64URL
PCA06	IdPAF	E	PCA03	C	1-1	43	Identificador único do PAF
PCA07	nRec	E	PCA03	N	1-1	15	número do recibo gerado pela SEF
PCA08	Signature	G	PCA01	XML	1-1	-	assinatura XML do grupo identificado pelo atributo Id

O campo PCA07, indicado na [Tabela 8.34](#), é gerado e fornecido pela SEF por meio do método [encaminharDFeRejeitado](#) ou [encaminharAutorizacoesRetidas](#).

8.8.3.2 Leiaute mensagem de retorno

Retorno: estrutura XML da mensagem de retorno para obter permissão para apagar autorizações retidas no DAF (veja [Tabela 8.35](#)).

Tabela 8.35: Leiaute da mensagem de retorno do método consultarAutorizacaoApagar

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
RCA01	retConsAutApagar	Raiz	-	-	-	-	TAG raiz
RCA02	versao	A	RCA01	C	1-1	4	versão do leiaute
RCA03	IdDAF	E	RCA01	C	1-1	22	Identificador único do DAF representado em Base64URL
RCA04	cStat	E	RCA01	N	1-1	3-4	código de <i>status</i> da resposta (veja Tabela 8.37)
RCA05	xMotivo	E	RCA01	C	1-1	1-255	descrição literal do <i>status</i> da resposta
RCA06	nRec	E	RCA01	N	0-1	15	número do recibo gerado pela SEF
RCA07	retDFe	G	RCA01	C	0-20	-	informações sobre o processamento do fragmento DAF
RCA08	chDFe	E	RCA07	C	0-1	44	chave de acesso do DF-e
RCA09	idAut	E	RCA07	C	0-1	43	identificador único da autorização
RCA10	hAut	E	RCA07	C	0-1	43	saída de uma função HMAC, representada em base64URL, que teve como chave a chave SEFAZ e como mensagem o idAut
RCA11	cStatAut	E	RCA07	N	1-1	3-4	código de <i>status</i> da resposta de autorização (veja Tabela 8.36)
RCA12	xMotAut	E	RCA07	C	1-1	1-255	descrição literal do <i>status</i> da resposta de autorização

8.8.3.3 Validações

Na Tabela 8.36 são apresentados os códigos de rejeição que poderão ser retornados após a validação do processamento do fragmento DAF.

Tabela 8.36: Códigos de rejeição sobre a validação do processamento do fragmento DAF

Código	Descrição
2003	valor do contador monotônico inválido
2004	assinatura de <i>token</i> inválida
2300	IdDAF do requerente não corresponde ao IdDAF de autorização do DF-e
2302	DAF deve atualizar a versão do software básico
2303	versão do software básico do DAF está desatualizada
2304	token de autorização inválido
2403	a rejeição informada para o DF-e é inválida
2404	as informações essenciais do DF-e são inválidas

Na Tabela 8.37 são apresentados os códigos de rejeição que poderão ser retornados após a aplicação das validações das regras de negócio.

Tabela 8.37: Códigos de rejeição da mensagem de entrada do método consultarAutorizacaoApagar

Código	Descrição
2000	registro do IdDAF não encontrado
2001	IdPAF não corresponde ao registro do DAF
2005	CNPJ do contribuinte diverge do CNPJ da assinatura
2006	IdPAF não registrado
2007	DAF extraviado
2009	DAF em situação irregular
2011	consumo indevido pelo aplicativo da empresa. Permitido no máximo 40 requisições por hora
2400	remoção extraordinária de autorização retida indisponível para o contribuinte
2401	número de recibo não encontrado
2402	lote em processamento

8.8.3.4 Final do processamento

Em caso de sucesso o processamento da consulta retorna o resultado da validação do fragmento **DAF**, o `cStatAut` com o valor 1005 e `cStat` com o valor 1000 da Tabela 8.4. Caso contrário resulta em uma mensagem de erro conforme Tabela 8.36 e Tabela 8.37.

8.9 Serviço Web - DAFAvisoExtravio

Para notificar à **SEF** de sinistro ocorrido com o **DAF**. Trata-se de um processo síncrono. O processo operacional está descrito na Subseção 7.6.6.

8.9.1 avisarExtravio

Função: notificar à **SEF** de sinistro ocorrido com o **DAF**.

8.9.1.1 Leiaute mensagem de entrada

Entrada: estrutura **XML** da mensagem de entrada de notificação de extravio do **DAF** (veja Tabela 8.38).

Tabela 8.38: Leiaute da mensagem de entrada do método avisarExtravio

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PAE01	pedExtravio	Raiz	-	-	-	-	TAG raiz
PAE02	versao	A	PAE01	C	1-1	4	versão do leiaute
PAE03	infExtravio	G	PAE01	-	1-1	-	informações da notificação de extravio do DAF
PAE04	Id	ID	PAE03	C	1-1	25	identificador da TAG a ser assinada. Deve-se informar o IdDAF , representado em Base64URL, precedida do literal DAF
PAE05	IdDAF	E	PAE03	C	1-1	22	Identificador único do DAF representado em Base64URL

PAE06	IdPAF	E	PAE03	C	1-1	43	Identificador único do PAF
PAE07	xJust	E	PAE03	C	1-1	15-255	descrição do sinistro ocorrido
PAE08	Signature	G	PAE01	XML	1-1	-	assinatura XML do grupo identificado pelo atributo Id

8.9.1.2 Leiaute mensagem de retorno

Retorno: estrutura XML da mensagem de retorno de notificação de extravio do DAF (veja Tabela 8.39).

Tabela 8.39: Leiaute da mensagem de retorno do método avisarExtravio

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
RAE01	retExtravio	Raiz	-	-	-	-	TAG raiz
RAE02	versao	A	RAE01	C	1-1	4	versão do leiaute
RAE03	IdDAF	E	RAE01	C	1-1	22	Identificador único do DAF representado em Base64URL
RAE04	cStat	E	RAE01	N	1-1	3-4	código de <i>status</i> da resposta (veja Tabela 8.40)
RAE05	xMotivo	E	RAE01	C	1-1	1-255	descrição literal do <i>status</i> da resposta

8.9.1.3 Validações

Na Tabela 8.40 são apresentados os códigos de rejeição que poderão ser retornados após a aplicação das validações das regras de negócio.

Tabela 8.40: Códigos de rejeição da mensagem de entrada do método avisarExtravio

2000	registro do IdDAF não encontrado
2001	IdPAF não corresponde ao registro do DAF
2005	CNPJ do contribuinte diverge do CNPJ da assinatura
2009	DAF em situação irregular
2010	justificativa inválida. A justificativa deve conter entre 15 e 255 caracteres
2011	consumo indevido pelo aplicativo da empresa. Permitido no máximo 40 requisições por hora
2500	notificação de extravio do DAF já foi realizada

8.9.1.4 Final do processamento

Em caso de sucesso o processamento da notificação de extravio do DAF retorna o cStat com o valor 1004 da Tabela 8.4. Caso contrário resulta em uma mensagem de erro conforme Tabela 8.40.

8.10 Serviço Web - DAFAlteracaoModoOperacao

Este serviço, composto pelos métodos `alterarModoOperacao` e `confirmarModoOperacao`, permite alterar o modo de operação do DAF. Trata-se de um processo síncrono. O processo operacional está descrito na Subseção 7.6.8.

8.10.1 alterarModoOperacao

Função: solicitar a alteração do modo de operação do DAF.

8.10.1.1 Leiaute mensagem de entrada

Entrada: estrutura XML da mensagem para a alteração do modo de operação do DAF (veja Tabela 8.41).

Tabela 8.41: Leiaute da mensagem de entrada do método `alterarModoOperacao`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PMO01	<code>pedModoOperacao</code>	Raiz	-	-	-	-	TAG raiz
PMO02	<code>versao</code>	A	PMO01	C	1-1	4	versão do leiaute
PMO03	<code>infModoOperacao</code>	G	PMO01	-	1-1	-	informações para a solicitação de alteração do modo de operação
PMO04	<code>Id</code>	ID	PMO03	C	1-1	25	identificador da TAG a ser assinada. Deve-se informar o <code>IdDAF</code> , representado em Base64URL, precedida do literal <code>DAF</code>
PMO05	<code>IdDAF</code>	E	PMO03	C	1-1	22	Identificador único do DAF representado em Base64URL
PMO06	<code>IdPAF</code>	E	PMO03	C	1-1	43	Identificador único do PAF
PMO07	<code>modoOp</code>	E	PMO03	B	1-1	1	modo de operação do DAF. Preencher com <code>false</code> em caso de DAF não compartilhado, um DAF por PDV; ou com <code>true</code> em caso de DAF compartilhado por mais de um PDV
PMO08	<code>xJust</code>	E	PMO03	C	1-1	15-255	justificativa da alteração do modo de operação
PMO09	<code>Signature</code>	G	PMO01	XML	1-1	-	assinatura XML do grupo identificado pelo atributo <code>Id</code>

8.10.1.2 Leiaute mensagem de retorno

Retorno: estrutura XML da mensagem de retorno da solicitação de alteração do modo de operação do DAF (veja Tabela 8.42).

Tabela 8.42: Leiaute da mensagem de retorno do método `alterarModoOperacao`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
RMO01	<code>retModoOperacao</code>	Raiz	-	-	-	-	TAG raiz
RMO02	<code>versao</code>	A	RMO01	C	1-1	4	versão do leiaute
RMO03	<code>IdDAF</code>	E	RMO01	C	1-1	22	Identificador único do DAF representado em Base64URL
RMO04	<code>cStat</code>	E	RMO01	N	1-1	3-4	código de <i>status</i> da resposta (veja Tabela 8.44)
RMO05	<code>xMotivo</code>	E	RMO01	C	1-1	1-255	descrição literal do <i>status</i> da resposta
RMO06	<code>tkDesafio</code>	E	RMO01	C	0-1	300-500	<i>token</i> JWT (veja Tabela 8.42)

O campo RMO06, indicado na Tabela 8.42, tem por objetivo conter um *token* JWT (veja Seção 8.3), cujo conteúdo (*payload*) está descrito na Tabela 8.43.

Tabela 8.43: Conteúdo do `tkDesafio` da mensagem de retorno do `alterarModoOperacao`

Nome do parâmetro	Tamanho (bytes)	Tipo	Descrição
<code>nnc</code>	22	<i>string</i>	valor aleatório gerado pela SEF representado em Base64URL

8.10.1.3 Validações

Na Tabela 8.44 são apresentados os códigos de rejeição que poderão ser retornados após a aplicação das validações das regras de negócio.

Tabela 8.44: Códigos de rejeição da mensagem de entrada do método `alterarModoOperacao`

Código	Descrição
2000	registro do <code>IdDAF</code> não encontrado
2001	<code>IdPAF</code> não corresponde ao registro do DAF
2005	<code>CNPJ</code> do contribuinte diverge do <code>CNPJ</code> da assinatura
2007	<code>DAF</code> extraviado
2010	justificativa inválida. A justificativa deve conter entre 15 e 255 caracteres
2011	consumo indevido pelo aplicativo da empresa. Permitido no máximo 40 requisições por hora
2600	o modo de operação já informado anteriormente

8.10.1.4 Final do processamento

Em caso de sucesso o processamento do pedido para alterar o modo de operação do `DAF` retorna um *nonce* gerado pela SEF e o `cStat` com o valor 1000 da Tabela 8.4. Caso contrário resulta em uma mensagem de erro conforme Tabela 8.44.

8.10.2 confirmarModoOperacao

Função: confirmar a alteração do modo de operação do `DAF`.

8.10.2.1 Leiaute mensagem de entrada

Entrada: estrutura XML da mensagem para alteração do modo de operação do `DAF` (veja Tabela 8.45).

Tabela 8.45: Leiaute da mensagem de entrada do método `confirmarModoOperacao`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PCM01	<code>pedConfModoOperacao</code>	Raiz	-	-	-	-	TAG raiz
PCM02	<code>versao</code>	A	PCM01	C	1-1	4	versão do leiaute
PCM03	<code>infConfModoOperacao</code>	G	PCM01	-	1-1	-	informações para a confirmação da alteração do modo de operação
PCM04	<code>Id</code>	ID	PCM03	C	1-1	25	identificador da TAG a ser assinada. Deve-se informar o <code>IdDAF</code> , representado em Base64URL, precedida do literal <code>DAF</code>

PCM05	IdDAF	E	PCM03	C	1-1	22	Identificador único do DAF representado em Base64URL
PCM06	IdPAF	E	PCM03	C	1-1	43	Identificador único do PAF
PCM07	tkAut	E	PCM03	C	1-1	400-600	token JWT (veja Tabela 8.46)
PCM08	Signature	G	PCM01	XML	1-1	-	assinatura XML do grupo identificado pelo atributo Id

O campo PCM07, indicado na Tabela 8.45, tem por objetivo conter um *token JWT* (veja Seção 8.3), cujo conteúdo (*payload*) está descrito na Tabela 8.46.

Tabela 8.46: Conteúdo tkAut da mensagem de entrada do confirmarModoOperacao

Nome do parâmetro	Tamanho (bytes)	Tipo	Descrição
daf	22	string	Identificador único do DAF representado em Base64URL
cnt	4	inteiro	valor atual do contador monotônico
mnc	22	string	valor aleatório gerado pela SEF representado em Base64URL

8.10.2.2 Leiaute mensagem de retorno

Retorno: estrutura XML da mensagem de retorno de confirmação da alteração do modo de operação do DAF (veja Tabela 8.47).

Tabela 8.47: Leiaute da mensagem de retorno do método confirmarModoOperacao

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
RCM01	retConfModoOperacao	Raiz	-	-	-	-	TAG raiz
RCM02	versao	A	RCM01	C	1-1	4	versão do leiaute
RCM03	IdDAF	E	RCM01	C	1-1	22	Identificador único do DAF representado em Base64URL
RCM04	cStat	E	RCM01	N	1-1	3-4	código de status da resposta (veja Tabela 8.49)
RCM05	xMotivo	E	RCM01	C	1-1	1-255	descrição literal do status da resposta
RCM06	tkModoOperacao	E	RCM01	C	0-1	300-500	token JWT (veja Tabela 8.48)

O campo RCM06, indicado na Tabela 8.47, tem por objetivo conter um *token JWT* (veja Seção 8.3), cujo conteúdo (*payload*) está descrito na Tabela 8.48.

Tabela 8.48: Conteúdo do tkModoOperacao da mensagem de retorno do confirmarModoOperacao

Nome do parâmetro	Tamanho (bytes)	Tipo	Descrição
mop	1	inteiro	modo de operação do DAF. 0 = DAF não compartilhado, um DAF por PDV; 1 = DAF compartilhado por mais de um PDV

8.10.2.3 Validações

Na Tabela 8.23 são apresentados os códigos de rejeição que poderão ser retornados após a aplicação das validações das regras de negócio.

Tabela 8.49: Códigos de rejeição da mensagem de entrada do método `confirmarModoOperacao`

Código	Descrição
2000	registro do <code>IdDAF</code> não encontrado
2001	<code>IdPAF</code> não corresponde ao registro do DAF
2002	<code>nonce</code> não corresponde ao informado pela <code>SEF</code>
2003	valor do <code>contador monotônico</code> inválido
2004	assinatura de <code>token</code> inválida
2005	<code>CNPJ</code> do contribuinte diverge do <code>CNPJ</code> da assinatura
2008	<code>IdDAF</code> do <code>token</code> não corresponde ao <code>IdDAF</code> informado
2011	consumo indevido pelo aplicativo da empresa. Permitido no máximo 40 requisições por hora

8.10.2.4 Final do processamento

Em caso de sucesso o processamento da confirmação da alteração do modo de operação do `DAF` retorna uma instrução para alteração e o `cStat` com o valor 1006 da [Tabela 8.4](#). Caso contrário, resulta em uma mensagem de erro conforme [Tabela 8.49](#).

8.11 Serviço Web - `DAFConsultaSB`

Este serviço permite ao PAF do contribuinte consultar a `SEF` sobre a versão atual do `Software Básico` disponibilizada pelo fabricante de seu `DAF`. Trata-se de um processo síncrono. O processo operacional está descrito na [Subseção 7.6.3](#).

8.11.1 `consultarVersaoSB`

Função: para consultar informações sobre a versão atual do `SB` disponibilizada pelo fabricante de seu `DAF`.

8.11.1.1 Leiaute mensagem de entrada

Entrada: estrutura `XML` da mensagem de entrada para consulta da versão do `SB` (veja [Tabela 8.50](#)).

Tabela 8.50: Leiaute da mensagem de entrada do método `consultarVersaoSB`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PCS01	<code>pedConsVersaoSB</code>	Raiz	-	-	-	-	TAG raiz
PCS02	<code>versao</code>	A	PCS01	C	1-1	4	versão do leiaute
PCS03	<code>infConsVersaoSB</code>	G	PCS01	-	1-1	-	informações para o consulta do <code>SB</code>
PCS04	<code>Id</code>	ID	PCS03	C	1-1	25	identificador da TAG a ser assinada. Deve-se informar o <code>IdDAF</code> , representado em <code>Base64URL</code> , precedida do literal <code>DAF</code>
PCS05	<code>IdDAF</code>	E	PCS03	C	1-1	22	Identificador único do <code>DAF</code> representado em <code>Base64URL</code>
PCS06	<code>IdPAF</code>	E	PCS03	C	1-1	43	Identificador único do <code>PAF</code>
PCS07	<code>modeloDaf</code>	E	PCS03	C	1-1	1-20	Nome do modelo <code>DAF</code>

PCS08	cnpjFabricante	E	PCS03	C	1-1	14	CNPJ do fabricante DAF
PCS09	Signature	G	PCS01	XML	1-1	-	assinatura XML do grupo identificado pelo atributo Id

8.11.1.2 Leiaute mensagem de retorno

Retorno: estrutura XML da mensagem de retorno da consulta da versão do SB (veja Tabela 8.51).

Tabela 8.51: Leiaute da mensagem de retorno do método consultarVersaoSB

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
RCS01	retConsVersaoSB	Raiz	-	-	-	-	TAG raiz
RCS02	versao	A	RCS01	C	1-1	4	versão do leiaute
RCS03	IdDAF	E	RCS01	C	1-1	22	Identificador único do DAF
RCS04	cStat	E	RCS01	N	1-1	3-4	código status da resposta (veja Tabela 8.52)
RCS05	xMotivo	E	RCS01	C	1-1	1-255	descrição literal do status da resposta
RCS06	dataSB	E	RCS01	D	0-1	-	data do lançamento da versão no formato "AAAA-MM-DD"
RCS07	versaoSB	E	RCS01	N	0-1	-	número da versão do SB
RCS08	urlSB	E	RCS01	C	0-1	15-2.000	URL onde o SB está disponível
RCS09	resumoCripSB	E	RCS01	C	0-1	43	resumo criptográfico do SB, representado em Base64URL

8.11.1.3 Validações

Na Tabela 8.52 são apresentados os códigos de rejeição que poderão ser retornados após a aplicação das validações das regras de negócio.

Tabela 8.52: Códigos de rejeição da mensagem de entrada do método consultarVersaoSB

Código	Descrição
2005	CNPJ do contribuinte diverge do CNPJ da assinatura
2006	IdPAF não registrado
2011	consumo indevido pelo aplicativo da empresa. Permitido no máximo 40 requisições por hora
2012	CNPJ do fabricante DAF inválido
2013	modelo DAF inválido

8.11.1.4 Final do processamento

Em caso de sucesso o processamento da consulta de SB retorna o resumo criptográfico do SB e o cStat com o valor 1003 da Tabela 8.4. Caso contrário resulta em uma mensagem de erro conforme Tabela 8.52.

8.12 Serviço Web - DAFAtualizacaoCertificado

Para obter a atualizar o [certificado digital da SEF](#) de um DAF. Trata-se de um processo síncrono. O processo operacional está descrito na [Subseção 7.6.7](#).

8.12.1 solicitarCertificado

Função: solicitar [certificado digital da SEF](#) para o modelo de DAF em questão.

8.12.1.1 Leiaute mensagem de entrada

Entrada: estrutura XML da mensagem de entrada da solicitação de atualização do certificado digital da SEF (veja [Tabela 8.53](#)).

Tabela 8.53: Leiaute da mensagem de entrada do método solicitarCertificado

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PSC01	pedCertificado	Raiz	-	-	-	-	TAG raiz
PSC02	versao	A	PSC01	C	1-1	4	versão do leiaute
PSC03	infCertificado	G	PSC01	-	1-1	-	informações sobre a solicitação do certificado digital da SEF
PSC04	Id	ID	PSC03	C	1-1	25	identificador da TAG a ser assinada. Deve-se informar o IdDAF, representado em Base64URL, precedida do literal DAF
PSC05	IdDAF	E	PSC03	C	1-1	22	Identificador único do DAF representado em Base64URL
PSC06	IdPAF	E	PSC03	C	1-1	43	Identificador único do PAF
PSC07	modeloDaf	E	PSC03	C	1-1	1-20	Nome do modelo DAF
PSC08	cnpjFabricante	E	PSC03	C	1-1	14	CNPJ do fabricante DAF
PSC09	Signature	G	PSC01	XML	1-1	-	assinatura XML do grupo identificado pelo atributo Id

8.12.1.2 Leiaute mensagem de retorno

Retorno: estrutura XML da mensagem de retorno da solicitação de atualização do certificado digital da SEF (veja [Tabela 8.54](#)).

Tabela 8.54: Leiaute da mensagem de retorno do método solicitarCertificado

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
RSC01	retCertificado	Raiz	-	-	-	-	TAG raiz
RSC02	versao	A	RCS01	C	1-1	4	versão do leiaute
RSC03	IdDAF	E	RSC01	C	1-1	22	Identificador único do DAF
RSC04	cStat	E	RSC01	N	1-1	3-4	código de <i>status</i> da resposta (veja Tabela 8.55)
RSC05	xMotivo	E	RSC01	C	1-1	1-255	descrição literal do <i>status</i> da resposta

RSC06 certificado E RCS01 C 0-1 1-2.000 novo certificado digital da SEF codificado no formato textual (veja (JOSEFSSON; LEONARD, 2015))

8.12.1.3 Validações

Na [Tabela 8.55](#) são apresentados os códigos de rejeição que poderão ser retornados após a aplicação das validações das regras de negócio.

Tabela 8.55: Códigos de rejeição da mensagem de entrada do método `solicitarCertificado`

Código	Descrição
2005	CNPJ do contribuinte diverge do CNPJ da assinatura
2006	IdPAF não registrado
2011	consumo indevido pelo aplicativo da empresa. Permitido no máximo 40 requisições por hora
2012	CNPJ do fabricante DAF inválido
2013	modelo DAF inválido

8.12.1.4 Final do processamento

Em caso de sucesso o processamento do pedido retorna um novo [certificado digital da SEF](#) e o `cStat` com o valor 1000 da [Tabela 8.4](#). Caso contrário resulta em uma mensagem de erro conforme [Tabela 8.55](#).

8.13 Serviço Web - DAFConsultaDispositivo

Para consultar a situação do DAF junto à SEF. Trata-se de um processo síncrono. O processo operacional está descrito na [Subseção 7.6.4](#).

8.13.1 consultarDispositivo

Função: consultar a situação do DAF junto à SEF.

8.13.1.1 Leiaute mensagem de entrada

Entrada: estrutura XML da mensagem de entrada de consulta do DAF (veja [Tabela 8.56](#)).

Tabela 8.56: Leiaute da mensagem de entrada do método `consultarDispositivo`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PID01	<code>pedSituacao</code>	Raiz	-	-	-	-	TAG raiz
PID02	<code>versao</code>	A	PID01	C	1-1	4	versão do leiaute
PID03	<code>infSituacao</code>	G	PID01	-	1-1	-	informações para a consulta do DAF
PID04	<code>Id</code>	ID	PID03	C	1-1	25	identificador da TAG a ser assinada. Deve-se informar o IdDAF, representado em Base64URL, precedida do literal DAF

PID05	IdDAF	E	PID03	C	1-1	22	Identificador único do DAF representado em Base64URL
PID06	IdPAF	E	PID03	C	1-1	43	Identificador único do PAF
PID07	Signature	G	PID01	XML	1-1	-	assinatura XML do grupo identificado pelo atributo Id

8.13.1.2 Leiaute mensagem de retorno

Retorno: estrutura XML da mensagem de retorno de consulta do DAF (veja Tabela 8.57).

Tabela 8.57: Leiaute da mensagem de retorno do método consultarDispositivo

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
RID01	retConsultaDAF	Raiz	-	-	-	-	TAG raiz
RID02	versao	A	RID01	C	1-1	4	versão do leiaute
RID03	IdDAF	E	RID01	C	1-1	36	Identificador único do DAF
RID04	cStat	E	RID01	N	1-1	3-4	código de <i>status</i> da resposta (veja Tabela 8.58)
RID05	xMotivo	E	RID01	C	1-1	1-255	descrição literal do <i>status</i> da resposta
RID06	IdPAF	E	RID01	C	1-1	43	Identificador único do PAF
RID07	ultimaVersaoSB	E	RID01	N	0-1	8	última versão disponível de SB
RID08	dataRegistro	E	RID01	D	0-1	-	Data de registro - Formato: "AAAA-MM-DD"
RID09	modeloDaf	E	RID01	C	1-1	0-20	Nome do modelo DAF
RID10	cnpjFabricante	E	RID01	C	0-1	14	CNPJ do fabricante DAF
RID11	cnpjContribuinte	E	RID01	C	0-1	14	CNPJ do contribuinte
RID12	cnpjResponsavel	E	RID01	C	0-1	14	CNPJ do responsável técnico
RID13	idCSRT	E	RID01	N	0-1	1	identificador do CSRT
RID14	xSituacao	E	RID01	C	0-1	1-255	descrição da situação do DAF junto à SEF (por exemplo: REGULAR, INATIVO, EXTRAVIADO)

8.13.1.3 Validações

Na Tabela 8.58 são apresentados os códigos de rejeição que poderão ser retornados após a aplicação das validações das regras de negócio.

Tabela 8.58: Códigos de rejeição da mensagem de entrada do método consultarDispositivo

Código	Descrição
2000	registro do IdDAF não encontrado
2001	IdPAF não corresponde ao registro do DAF
2005	CNPJ do contribuinte diverge do CNPJ da assinatura
2009	DAF em situação irregular
2011	consumo indevido pelo aplicativo da empresa. Permitido no máximo 40 requisições por hora

8.13.1.4 Final do processamento

Em caso de sucesso, retorna as informações referente ao DAF e o cStat com o valor 1000 da [Tabela 8.4](#). Caso contrário, resulta em uma mensagem de erro conforme [Tabela 8.58](#).

8.14 Serviço Web - DAFSolicitacaoChavePAF

Para recuperar a [chave PAF](#) que está associada a um determinado [DAF](#). Necessário somente se o PAF vier a perder a [chave PAF](#) que foi gerada no processo de registro de DAF (veja [Seção 5.1](#)). Trata-se de um processo síncrono. O processo operacional está descrito na [Subseção 7.6.5](#).

8.14.1 solicitarChavePAF

Função: solicitar a [chave PAF](#) que está associada a um determinado [DAF](#).

8.14.1.1 Leiaute mensagem de entrada

Entrada: estrutura [XML](#) da mensagem de entrada de solicitação de [chave PAF](#) (veja [Tabela 8.59](#)).

Tabela 8.59: Leiaute da mensagem de entrada do método `solicitarChavePAF`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PCP01	pedChavePAF	Raiz	-	-	-	-	TAG raiz
PCP02	versao	A	PCP01	C	1-1	4	versão do leiaute
PCP03	infChavePAF	G	PCP01	-	1-1	-	informações para solicitação da chave PAF
PCP04	Id	ID	PCP03	C	1-1	25	identificador da TAG a ser assinada. Deve-se informar o IdDAF, representado em Base64URL, precedida do literal <i>DAF</i>
PCP05	IdDAF	E	PCP03	C	1-1	22	Identificador único do DAF representado em Base64URL
PCP06	IdPAF	E	PCP03	C	1-1	43	Identificador único do PAF
PCP07	Signature	G	PCP01	XML	1-1	-	assinatura XML do grupo identificado pelo atributo Id

8.14.1.2 Leiaute mensagem de retorno

Retorno: estrutura [XML](#) da mensagem de retorno de solicitação de [chave PAF](#) (veja [Tabela 8.60](#)).

Tabela 8.60: Leiaute da mensagem de retorno do método `solicitarChavePAF`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
RCP01	retChavePAF	Raiz	-	-	-	-	TAG raiz
RCP02	versao	A	RCP01	C	1-1	4	versão do leiaute
RCP03	IdDAF	E	RCP01	C	1-1	22	Identificador único do DAF representado em Base64URL
RCP04	cStat	E	RCP01	N	1-1	3-4	código de <i>status</i> da resposta (veja Tabela 8.61)

RCP05	xMotivo	E	RCP01	C	1-1	1-255	descrição literal do <i>status</i> da resposta
RCP06	chavePAF	E	RCP01	C	0-1	86	chave PAF representada em Base64URL

8.14.1.3 Validações

Na [Tabela 8.61](#) são apresentados os códigos de rejeição que poderão ser retornados após a aplicação das validações das regras de negócio.

Tabela 8.61: Códigos de rejeição da mensagem de entrada do método `solicitarChavePAF`

Código	Descrição
2000	registro do IdDAF não encontrado
2001	IdPAF não corresponde ao registro do DAF
2005	CNPJ do contribuinte diverge do CNPJ da assinatura
2006	IdPAF não registrado
2009	DAF em situação irregular
2011	consumo indevido pelo aplicativo da empresa. Permitido no máximo 40 requisições por hora

8.14.1.4 Final do processamento

Em caso de sucesso o processamento retorna uma nova [chave PAF](#) e o `cStat` com o valor 1000 da [Tabela 8.4](#). Caso contrário resulta em uma mensagem de erro conforme [Tabela 8.61](#).

Referências

- ANSI. *Public Key Cryptography for the Financial Services Industry Key Agreement and Key Transport Using Elliptic Curve Cryptography*. Nov. 2001. Disponível em: <<https://standards.globalspec.com/std/26827/X9.63>>. Acesso em: 12 fev. 2021.
- BRADNER, Scott. *Key words for use in RFCs to Indicate Requirement Levels*. Mar. 1997. Disponível em: <<https://tools.ietf.org/html/rfc2119>>.
- BRAY, T. *The JavaScript Object Notation (JSON) Data Interchange Format*. Dez. 2017. Disponível em: <<https://tools.ietf.org/html/rfc8259>>.
- BRAY, T. et al. *Extensible Markup Language (XML) 1.0 (Fifth Edition)*. Nov. 2008. Disponível em: <<https://www.w3.org/TR/2008/REC-xml-20081126>>.
- CONFAZ (Ed.). *Ajuste SINIEF 15/18*. Nov. 2018. Disponível em: <https://www.confaz.fazenda.gov.br/legislacao/ajustes/2018/AJ0015_18>. Acesso em: 28 abr. 2020.
- COOK, Steve et al. *Unified Modeling Language (UML) Version 2.5.1*. Dez. 2017. Disponível em: <<https://www.omg.org/spec/UML/2.5.1>>.
- COOPER, D. et al. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. Mai. 2008. Disponível em: <<https://tools.ietf.org/html/rfc5280>>.
- ENCAT. *Manual de Orientação do Contribuinte - versão 7.02*. Mai. 2019a. Disponível em: <<https://dfe-portal.svrs.rs.gov.br/Nfe/Documentos#>>.
- _____. *Manual de Orientações do Contribuinte do BP-e, versão 1.00b*. Abr. 2019b. Disponível em: <<https://dfe-portal.svrs.rs.gov.br/Bpe/Documentos#>>.
- _____. *Manual de Padrões Técnicos da Contingência Offline para NFC-e - versão 2.0*. Dez. 2016. Disponível em: <<http://www.nfe.fazenda.gov.br/portal/exibirArquivo.aspx?conteudo=YbZEjEHCuHQ=>>>.
- _____. *Nota Técnica 2018.005 - Alteração do leiaute da NF-e/NFC-e - v 1.30*. Abr. 2019c. Disponível em: <<http://www.nfe.fazenda.gov.br/portal/exibirArquivo.aspx?conteudo=KgqR7PT4Vv4=>>>.
- ICP-BRASIL (Ed.). *DOC-ICP-01 - Padrões e Algoritmos Criptográficos da ICP-Brasil, V.5.2*. Out. 2019. Disponível em: <https://antigo.iti.gov.br/images/repositorio/legislacao/documentos-principais/01.1/DOC-ICP-01.01_-_v.4.2_PADROES_E_ALGORITMOS_CRIPTOGRAFICOS_DA_ICP-BRASIL_copy.pdf>.
- _____. *DOC-ICP-04 - Requisitos mínimos para as políticas de certificados na ICP-Brasil, V.7.2*. Abr. 2020. Disponível em: <https://antigo.iti.gov.br/images/repositorio/legislacao/documentos-principais/04/DOC-ICP-04_-_v.7.2_-_REQUISITOS_MINIMOS_PARA_PC.pdf>.
- JONES, M. *JSON Web Algorithms (JWA)*. Mai. 2018. Disponível em: <<https://tools.ietf.org/html/rfc7518>>.
- _____. *JSON Web Encryption (JWE)*. Mai. 2015a. Disponível em: <<https://tools.ietf.org/html/rfc7516>>.

JONES, M. *JSON Web Key (JWK)*. Mai. 2015b. Disponível em: <<https://tools.ietf.org/html/rfc7517>>.

JONES, M.; BRADLEY, J.; SAKIMURA, N. *JSON Web Token (JWT)*. Mai. 2015. Disponível em: <<https://tools.ietf.org/html/rfc7519>>.

JOSEFSSON, S. *The Base16, Base32, and Base64 Data Encodings*. Out. 2006. Disponível em: <<https://tools.ietf.org/html/rfc4648>>.

JOSEFSSON, S.; LEONARD, S. *Textual Encodings of PKIX, PKCS, and CMS Structures*. Abr. 2015. Disponível em: <<https://tools.ietf.org/html/rfc7468>>.

KRAWCZYK, Hugo; BELLARE, Mihir; CANETTI, Ran. *HMAC: Keyed-Hashing for Message Authentication*. Fev. 1997. Disponível em: <<https://tools.ietf.org/html/rfc2104>>.

LEACH, Paul J.; MEALLING, Michael; SALZ, Rich. *A Universally Unique Identifier (UUID) URN Namespace*. Jul. 2005. Disponível em: <<https://tools.ietf.org/html/rfc4122>>.

MORIARTY, K. et al. *PKCS #1: RSA Cryptography Specifications Version 2.2*. Nov. 2016. Disponível em: <<https://tools.ietf.org/html/rfc8017>>.

NIST. *Digital Signature Standard*. National Institute of Standards e Technology, jul. 2013. Federal Information Processing Standards Publications (FIPS PUBS) 186-4. Disponível em: <<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>>.

_____. *Secure Hash Standards*. National Institute of Standards e Technology, ago. 2015. Federal Information Processing Standards Publications (FIPS PUBS) 180-4. Disponível em: <<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>>.

NYSTROM, M.; KALISKI, B. *PKCS #10: Certification Request Syntax Specification Version 1.7*. Nov. 2000. Disponível em: <<https://tools.ietf.org/html/rfc2986>>.

RESCORLA, Eric. *The Transport Layer Security (TLS) Protocol Version 1.3*. Ago. 2018. Disponível em: <<https://tools.ietf.org/html/rfc8446>>.

USB-IF. *Universal Serial Bus Class Definitions for Communications Devices*. USB-IF, nov. 2010. Revision 1.2 (Errata 1.0).

_____. *Universal Serial Bus Communication Class Subclass Specification for PSTN Devices*. USB-IF, fev. 2007. Revision 1.2.

W3C. *SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)*. Abr. 2007. <http://www.w3.org/TR/soap12>.

Apêndices


```

UFNUPjAuMDA8L3ZGQ1BTVD48dkZDUFNUUmVOPjAuMDA8L3ZGQ1BTVFJldD48d1Byb2Q-MjI5LjkwPC92UHJvZD48dkZy
ZXR1PjAuMDA8L3ZGcmVOZT48d1N1Zz4wLjAwPC92U2VnPx2RGVzYz4wLjAwPC92RGVzYz48dk1JPjAuMDA8L3ZJST48
dk1QST4wLjAwPC92SVBJPjx2SVBJRGV2b2w-MC4wMDwvdKlQSURldm9sPjx2UE1TPjAuMDA8L3ZQSVm-PhZDT0ZJT1M-
MC4wMDwvdKlNPRk1OUz48dk91dHJvPjAuMDA8L3ZPdXRybz48dk5GPjIyOS45MDwvdKl5GPjx2VG90VHJpYj44Ny42NDwv
d1RvdFRyaWI-PC9JQ01TVG90PjwvdG90YWw-PC9pbmZORmU- ",
4 "hdf": "JNlaRI8G_J4WK5AIjwQ9jhrw1oa4M_cd_eNtS7ouuQ8",
5 "pdv": "x4YowJo6Xs"
6 "red": "U3EXAXPbu2ApHg7-Z01MNBzuQQyGCZ-vfnJe9eGw_QA"
7 }

```

A.2 Respostas sem assinatura digital

A Listagem A.3 apresenta a representação de uma resposta do DAF que não contém assinatura digital e não contém parâmetros adicionais. Na resposta DEVE conter apenas a chave `res` com o valor de acordo com a Tabela 6.2.

Listagem A.3: Documento JSON para respostas sem assinatura digital e sem parâmetros

```

1 {
2   "res": 0
3 }

```

A Listagem A.4 apresenta a representação de uma resposta do DAF que não contém assinatura digital e contém parâmetros adicionais. Na resposta DEVE conter a chave `res` com o valor 0, seguido dos parâmetros na sequência em que eles aparecem nas suas respectivas tabelas na Subseção 6.1.2.

Listagem A.4: Documento JSON para respostas sem assinatura digital e com parâmetros adicionais

```

1 {
2   "res": 0,
3   "daf": "YRaQYtWtROCSI-gCuL7oyg",
4   "mop": 0,
5   "vsb": 2,
6   "hsb": "MoxgVDBf9MdYEQtb97TGchVvA8mh3gkjBE-C2-mzviU",
7   "fab": "86096781000185",
8   "mdl": "modelo-daf",
9   "cnt": 0,
10  "crt": "-----BEGIN CERTIFICATE-----\
nMIIFdDCCA1ygAwIBAgIUfktOTKkRrLIELtjWwcnPwoYzrPMwDQYJKoZIhvcNAQEL\
nBQAwdDEMMAoGA1UECgwDU0VGMQ4wDAYDVQQQLDAVHRVNBQzELMAkGA1UEBhMCQ1Ix\
nFzAVBgNVBAGMD1NhbnRhIENhdGFyaW5hMRYwFAYDVQQHDA1GbG9yaWFub3BvbG1z\
nMRYwFAYDVQQDDA1zZWYuc2MuZ292LmJyMB4XDTEwMDUxNzE3MDg3N1oXDTEwMDUx\
nNjE3MDg3N1owDQYwDQYwDQYwDQYwDQYwDQYwDQYwDQYwDQYwDQYwDQYwDQYw\
nBhMCQ1IxZzAVBgNVBAGMD1NhbnRhIENhdGFyaW5hMRYwFAYDVQQHDA1GbG9yaWFu\
nb3BvbG1zMRYwFAYDVQQDDA1zZWYuc2MuZ292LmJyMIIICjANBgkqhkiG9w0BAQEF\
nAAOCAG8AMIICGKCAgEAY3ONtcsL6GfUXtRV4Z1B1L1teLRXYvJPz8N4tgnlWJSa\nKdGZ9XiQ2rz7UFDAM+
Oy08EW7s10ieK3PKsjKxEUE9krA57UinsRu0FQ+pJ/fZYc\nGQRCC/
U0EztrXpIcjaD55zFqbpYyEtDMGPRahC5ToT0bbd1863Zg/VJTedyTYG\nY/rLw+f5dhgTMQy/pmb4f0hv6k/
MDzfjSUqdTMR1U51FRYmFzo38eJd0sk3ABmul\nIfSes0Iq2l/qjqdi5Z1QiKoUVnA2F57qYG8CYrmKSQMzq+xw+
iI934Gbou+Nv11/\nExFIJEiFvU107S+dBv6XaleUUJfVD/QORzo3Yma5ur/Yfn+68E41SZCOI3jz//1b\
ni2jutZWAHOCdmfn95bYCAadmM4j1jven4fsc1+dakYemZ1aYyoqhM4cCfAURIZjqC\
ndFLB6kay5GAE7yn55FytNtGX10BSdqfv4V/UDaePjPeG5hcVZGVuLjNeTYsqdHV\

```

```

nEGOHYJzZsovfhF332JtK1feOp94x2QjeGNGOgg2uyjN14S6qmBd49+E0/W4Q7rI2\nf+yJjJK+8ZE2dgmImJ+6
rHVt0tiSbtzI6fcrY9ZRcuVGPmCGFSMNHzv7fh21D1f\n3txog99x7IelG6fBfCF0EHmj4/
dJoWdVtwc1F2IIRU6c1sn5nF7P+YfsCdBYFxCUC\nAwEAATANBgkqhkiG9wOBAQsFAAOCAGeAAbbr8o0bk0/
wGdVkBpKamCfQ1XfK1JZ+M\nnbBQmSVfIYP7jfQaijYFSGe/GZRnsaTvMAE3bElmUcEzKwZMMdib4RB0VINsyhju\
n2BpiB3STp3ybXgdNKLXxhokN9++eqFszntbJlIAnNEwlllu6cbBHXAemsPQ3y05En\
nTmyeIHnsqCeHqToyehb9B1n4DyRG2oHhV7i31V55MFAZOTRxoUR/Og45mUNNQcv5\nvkdTD/
LczBVjT9qe3D0pHHWDHP6a+N14I8bsYC+h7+yK00eeSJU08UrtJ/oXBoF8a\npNhFEE+
dv5ZJ0oPSP4mPVsDD799zdyDl9af/NBBzvXLeMaOUCLWuU0Vcj0y5hWDH\nn+Xp7s9RZULGc122ZEbhunxUi/
TechPLPs4TRDg3b3f68jaULQzsfhiamS6Vn+kSh\n1rytea5sHs49B+3
W6Fv128GjR8gGcYwQFOFBbD8GFsHHYefsMmilEdw0m/jq3IAI\nDnvRQNFpN5gW9RS1Y2GNQs1k03eTmDX+eeG+qhcX+
fRF8C2V1pcgNcl0vXew0A0xf\nVDHD/MCwvk/xU2ZSxzJ8abtQFBrrAbZBq2c44DmFz44NN1aG91CDMOXPifUy1cr1\
njmGZr7CdyL49qcsf8Js0h0o0eZqTsSgHWJfL4W2IpHG/9V1p7ZfyLu8WeMHMrhZa\nk041Z8/+MXs=\n-----END
CERTIFICATE-----\n",
11 "est": "inativo",
12 "mxd": 1000,
13 "ndf": 0,
14 "rts": []
15 }

```

A.3 Pedidos com assinatura digital

A Listagem A.5 apresenta a representação de um pedido para o DAF que contém uma assinatura digital. O documento JSON DEVE conter apenas a chave `cmd` com o valor de acordo com a Tabela 6.1 e a chave `jwt` que contém como valor um `token` JWT.

Listagem A.5: Documento JSON para pedidos com assinatura digital

```

1 {
2   "msg": 1,
3   "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJub25jZSI6Im43TlN1VDNCLWxJZk1UbWFPaDdSY3cifQ.
   Ds8lH01j-u_1IJecMxz1_2TZ4Xc9aA11fgZa7yAFZpjtNo0bkoSbZqb8B3qwcJrAXq97SJIJLsnKP36q2TjDDhPpDo
   zoVq2End0_Qn9IFbZFPsZaaXUx04ze86LXyXln8R-B0f2y3n4ueyMs9lGwf-ihIRgcHSvz3nTtv39-F-M9bHhQ8I9l
   LtUtz47XXzEhjIZPZwj0iH0xgRJdkSNt07pVbJP6_nYOUTekcYGx1EATkPxmTH4AEcjQ5x8eq5PUDCpXCzXE6wX_cy
   hNp-3uIghoF9-5RHMerIg4526_nGrMiPDABFv0GiX-xgIO-m43UUyhRKRrec3nV624pZhVMg"
4 }

```

A.4 Respostas com assinatura digital

A Listagem A.6 apresenta a representação de uma resposta do DAF que contém uma assinatura digital. O documento JSON DEVE conter apenas a chave `res` com o valor 0 e a chave `jwt` que contém como valor um `token` JWT.

Listagem A.6: Documento JSON para respostas com assinatura digital

```

1 {
2   "res": 0,
3   "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJub25jZSI6Im43TlN1VDNCLWxJZk1UbWFPaDdSY3cifQ.
   Ds8lH01j-u_1IJecMxz1_2TZ4Xc9aA11fgZa7yAFZpjtNo0bkoSbZqb8B3qwcJrAXq97SJIJLsnKP36q2TjDDhPpDo
   zoVq2End0_Qn9IFbZFPsZaaXUx04ze86LXyXln8R-B0f2y3n4ueyMs9lGwf-ihIRgcHSvz3nTtv39-F-M9bHhQ8I9l
   LtUtz47XXzEhjIZPZwj0iH0xgRJdkSNt07pVbJP6_nYOUTekcYGx1EATkPxmTH4AEcjQ5x8eq5PUDCpXCzXE6wX_cy
   hNp-3uIghoF9-5RHMerIg4526_nGrMiPDABFv0GiX-xgIO-m43UUyhRKRrec3nV624pZhVMg"

```

```
4 }
```

A.5 Como representar chave pública RSA no *Header* de um *token* JWT

A Listagem A.7 apresenta a representação do cabeçalho (*header*) do *token* JWT quando o mesmo for assinado com uma chave RSA e a chave pública par da chave privada que assinou o *token* for transportada no cabeçalho. No documento JSON DEVEM estar presentes as chaves *typ*, *alg* e *jwk*. O valor da chave *jwk* DEVE ser um documento JSON e DEVEM estar presentes as chaves *kt**y*, *n* e *e*.

Listagem A.7: Documento JSON com o *header* do *token* JWT utilizando chave RSA

```
1 {
2   "typ": "JWT",
3   "alg": "RS256",
4   "jwk": {
5     "kty": "RSA",
6     "n": "pAn88H6-v2e_o1COYsH8tj10nNAPxQhTuv9ZwxctZasmGgjQjkr_XPgfEVuuJk1T1Gf5Bko5A1-zWUmICoRtn
7     Efw_mt0onjPxID-A_qzeMq0XfDZGyrSmH9PK1CNPvFenS7b_j8Rp2y1qzQ58Ez92bUPUEBG3UHcnBBz7cR47MA36yN
8     B5sQGveroMQXsRK4eo8wuLoBvts0w85qXKToMigyXpPt6k3mpFEDmQ-p4RGNCwzakcmnodwUMbRdXSXYvXaVEu0gk0
9     lUvJgTxm8Bbj20xoKbKpaqtt9spCm6byqb-4Fh04-nvYh0sJ2n0NmdYLI3hD7N1h6RHbAYwLdl_Sw",
10    "e": "AQAB"
11  }
12 }
```

A.6 Como representar chave pública EC no *Header* de um *token* JWT

A Listagem A.7 apresenta a representação do cabeçalho (*header*) do *token* JWT quando o mesmo for assinado com uma chave EC e a chave pública par da chave privada que assinou o *token* for transportada no cabeçalho. No documento JSON DEVEM estar presentes as chaves *typ*, *alg* e *jwk*. O valor da chave *jwk* DEVE ser um documento JSON e DEVEM estar presentes as chaves *crv*, *x*, *y* e *kt**y*.

Listagem A.8: Documento JSON com o *header* do *token* JWT utilizando chave EC

```
1 {
2   "typ": "JWT",
3   "alg": "ES256",
4   "jwk": {
5     "crv": "P-256",
6     "kty": "EC",
7     "x": "BCOFs7eAkxsJ9b2XZ147ScbLicZm0QJfyzmNcm8NAIE",
8     "y": "C3L2m0FeZEV5b4aoULvtgX5zKeZcrT5U1bcTZeUydtE"
9   }
10 }
```

A.7 Como representar a chave SEF cifrada utilizando *token* JWE

A Listagem A.9 apresenta a representação do cabeçalho (*header*) do *token* JWE. No documento JSON DEVEM estar presentes as chaves *alg*, *enc* e *epk*. O valor da chave *epk* DEVE ser um documento

JSON e DEVEM estar presentes as chaves `crv`, `kty`, `x` e `y`. A chave pública EC transportada dentro da chave `epk` do header do *token* *JWE* é uma chave efêmera (temporária) compartilhada entre DAF e SEF, e deve ser usada para decifrar a *chave* SEF.

Listagem A.9: Documento JSON com o *header* do *token* *JWE*

```
1 {
2   "alg": "ECDH-ES",
3   "enc": "A128CBC-HS256",
4   "epk": {
5     "crv": "P-256",
6     "kty": "EC",
7     "x": "0Uj5oFqfK4ZCpKfYowCNfrCOoTnPvPCjolbXixMST1g",
8     "y": "zQH2DuwSV7KipPpPVV7yEfiRb0ZUHTKBHZSdb3xpLDY"
9   }
10 }
```

B Exemplos de mensagens por processo operacional com o DAF

Neste capítulo são apresentados exemplos de mensagens do DAF e serviços providos pela SEF. Organizados por processo operacional, os exemplos apresentados nesse apêndice possuem quebras de linha e espaços em branco somente para facilitar a leitura dos mesmos.

B.1 Registro do DAF junto à SEF

Os exemplos apresentados referem-se as mensagens ilustradas no diagrama de sequência apresentado na [Figura 5.1](#). O processo operacional é detalhado na [Seção 5.1](#) e fluxos alternativos e de exceção para esse processo são apresentados nos Casos de Uso [UC-4.10](#) e [UC-4.7](#).

B.1.1 Mensagem DAF consultarInformacoes

B.1.1.1 Pedido - mensagem 2

Listagem B.1: Documento JSON para o pedido da mensagem consultarInformacoes

```
1 {  
2   "msg": 8  
3 }
```

B.1.1.2 Resposta - mensagem 3

Listagem B.2: Documento JSON para a resposta da mensagem consultarInformacoes

```
1 {  
2   "res": 0,  
3   "daf": "YRaQYtWtROCSI-gCuL7oyg",  
4   "mop": 0,  
5   "vsb": 2,  
6   "hsb": "MoxgVDBf9MdYEQtB97TGchVvA8mh3gkjBE-C2-mzviU",  
7   "fab": "86096781000185",  
8   "mdl": "modelo-daf",  
9   "cnt": 0,  
10  "crt": "-----BEGIN CERTIFICATE-----\  
      nMIIFdDCCA1ygAwIBAgIUfktOTKkRrLIELtjWwcnPwoYzrPMwDQYJKoZIhvcNAQEL\  
      nBQAwdDEMMAoGA1UECgwDUOVGMQ4wDAYDVQQQLDAVHRVNBQzELMAkGA1UEBhMCQ1Ix\  
      nFzAVBgNVBAGMD1NhbnRlIENhdGFyaW5hMRYwFAFDVQZHDA1GbG9yaWFub3BvbG1z\  
      -----"
```

```

nMRYwFAYDVQDDA1zZWYuc2MuZ292LmJyMB4XDTIxMDUxNzE3MDgxN1oXDTMxMDUx\
nNjE3MDgxN1owdDEMMAoGA1UECgwDUOVGMQ4wDAYDVQQLDAVHRVNBQzELMAkGA1UE\
nBhMCQlIxZzAVBgNVBAGMD1NhbhRhIENhdGFyaW5hMRyYwFAYDVQQA1G9yaW5u\
nb3BvbG9yaW5uFAYDVQDDA1zZWYuc2MuZ292LmJyMIIICjANBgkqhkiG9w0BAQEF\
nAAOCAG8AMIIICCgKCAgEay30NtcsL6GfUXtRV4Z1B1L1teLRXyVJPz8N4tgnlWJSa\nKdGZ9XiQ2rz7UfDAM+
Oy08EW7s10ieK3PKsjKxEUE9krA57UinsRu0FQ+pJ/fZyC\nGQrCC/
UOEzrRXpIcjad55zFqbpYyEtdMGPRahC5ToT0bbd1863Zg/VJTedxYTYG\nY/r1W+f5dhgTMQy/pmb4f0hv6k/
MDzfjSUqdTMR1U51FRYmFzo38eJd0sk3ABmul\nIfSes0Iq2l/qjqdi5Z1QiKoUVnA2F57qYG8CYrmKSMzq+xw+
iI934Gbou+Nv11/\nExFIJEiFvU107S+dBv6XaleUUJfVD/QORzo3Yma5ur/Yfn+68E41SZCOI3jz//1b\
ni2jutZWAHOCdmfn95bYCAAdm4jljven4fsc1+dakYemZ1aYyoqhM4cCfAURIZjqC\
ndFLB6kay5GAE7yn55FytNtGX10BSdqfv4V/UDaePjPeG5hcVZGVuLjNeTYsqdHV\
nEGOHYJzZsovfhF332JtK1fe0p94x2QjeGNGOgg2uyjN14S6qmBd49+EO/W4Q7rI2\nf+yJjJK+8ZE2dgmImJ+6
rHVt0tiSbtzI6fcrY9ZrcuvGPGMCGFSMNHzv7fh21D1f\n3txog99x7IelG6fBfCFOEHmj4/
dJowDvtwc1F2IIRU6c1sn5nF7P+YfsCdBYfXUC\nAwEAATANBgkqhkiG9w0BAQsFAAOCAGEAAbbr8o0bk0/
wGdVkBpKamCfQ1XfK1JZ+M\nbBQmSVfIYP7jfqaijYFSGe/GZRnsaTvMAE3bElmUcEzKwZMMdib4RB0VINsyhju\
n2BpiB3STp3ybXgdNKLXxhokN9++eqFszntbJlIAnNEw1lu6cbBHXAemsPQ3y05En\
nTmyeIHnsqCeHqToyehb9B1n4DyRG2oHhV7i31V55MFAZOTRxoUR/Og45mUNNQcv5\nvkvTD/
LczBVjT9qe3D0pHHWDHP6a+N14I8bsYC+h7+yK00eesJU08UrtJ/oXBof8a\nnpNhFEE+
dv5ZJ0oPSP4mPvsDD799zdyD19af/NBBzvxLeMaOUCLWuU0Vcj0y5hWDH\nn+Xp7s9RZULGc122ZEbhunxUi/
TechPLPs4TRDg3b3f68jaULQzsfhiamS6Vn+kSh\n1rytea5sHs49B+3
W6Fv128GjR8gGcYwQFOFBbD8GFsHHYEfsMmilEdw0m/jq3IAI\nNdvrQNFpN5gW9RS1Y2GNQs1k03eTmDX+eeG+qhcX+
fRF8C2VlpcgNcl0vXew0A0xf\nnVDHD/MCwvk/xU2ZSxzJ8abtQFBrrAbZBq2c44DmFz44NN1aG91CDMOXPifUy1cr1\
nJmGZr7CdyL49qcsf8Js0h0o0eZqTsSgHWJfL4W2IpHG/9V1p7ZfyLu8WeMHMrhZa\nk041Z8/+MXs=\n-----END
CERTIFICATE-----\n",

```

```

11 "est": "inativo",
12 "mxd": 1000,
13 "ndf": 0,
14 "rts": []
15 }

```

B.1.2 Serviço SEF DAFRegistroDispositivo - método iniciarRegistro

B.1.2.1 Entrada - mensagem 4

Listagem B.3: Documento XML de entrada do método iniciarRegistro

```

1 <iniciarRegistro xmlns="http://www.portalfiscal.inf.br/daf/wsd/DAFRegistroDispositivo">
2   <pedRegistro versao="1.00" xmlns="http://www.portalfiscal.inf.br/daf">
3     <infRegistro Id="DAFYRaQYtWtROCSI-gCuL7oyg">
4       <idDAF>YRaQYtWtROCSI-gCuL7oyg</idDAF>
5       <idPAF>3BV9hxwDWDkzQf2R6hEqHfNevwsuRtVwEHfJto9N0qE</idPAF>
6       <modeloDaf>modelo-daf</modeloDaf>
7       <cnjFabricante>86096781000185</cnjFabricante>
8       <cnjContribuinte>28572444000110</cnjContribuinte>
9       <cnjResponsavel>87528541000175</cnjResponsavel>
10      <idCSRT>1</idCSRT>
11      <modoOp>>false</modoOp>
12    </infRegistro>
13    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><!-- Assinatura --></Signature>
14  </pedRegistro>
15 </iniciarRegistro>

```

B.1.2.2 Retorno - mensagem 5

A SEF irá gerar um *token* JWT que deverá ser incorporado no documento XML do retorno. A Listagem B.4 apresenta o cabeçalho e o conteúdo (veja Tabela 6.3) para a geração do *token* JWT. Neste exemplo, o *token* JWT é assinado com a chave privada da SEF (chave RSA) par da chave pública contida no certificado digital da SEF que está presente no DAF. O retorno da SEF é apresentado na Listagem B.5 e o *token* JWT gerado a partir da Listagem B.4 pode ser encontrado dentro do campo tkDesafio.

Listagem B.4: Cabeçalho e conteúdo do *token* JWT que será incorporado no retorno do método iniciarRegistro

```
1 {
2   "typ": "JWT",
3   "alg": "RS256"
4 }
5 {
6   "nnc": "snvhgXNfz6H80H91BNt4kg"
7 }
```

Listagem B.5: Documento XML de retorno do método iniciarRegistro

```
1 <iniciarRegistroResponse xmlns="http://www.portalfiscal.inf.br/daf/wsd/DAFRegistroDispositivo">
2   <retRegistro versao="1.00" xmlns="http://www.portalfiscal.inf.br/daf">
3     <idDAF>YRaQYtWtROCSI-gCuL7oyg</idDAF>
4     <cStat>1000</cStat>
5     <xMotivo>Solicitação recebida com sucesso</xMotivo>
6     <tkDesafio>eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJubmMiOiJzbnZoZ1h0Zno2SDgwSDlsQk50NGtnIn0.
7     TJg17N31-6K0xizFe81o0dGEKQzIft3BSRGoFbWE7QQeBEHdbvbZ57ik4HjLpBytSyBqpjouukXfbizSEaAMZUBApft
8     XBfBjUL5RzQH66n9r0x08QCYWECG-12Pri9j2b7k5FbjinLSNia0sTaDk0EcNSi2muJsH6131IY4sXDJQcNNCAkaunS
9     pAz5SjUstfnuCFKriK9jNOjWQTGntQRC_A6cY_A1FrLxinLpl-b0fuNLk06INvutKgEqen-LCrWRM8CZava0VqLFAai
10    tJgvDic0qITqHd-iZg97IPp3PdjofOKAk0ci_gIEryHx31U_j9i1U9Tjp31D-nm4ISSKh3jHx5KrRvGDdw09rzpprzm
11    Lapc-Ub8QJtgxVgcr-__NHvg_9RfT1CEwGeOELRNsLW-Hs0p03kHc_-yXnmm0oD-GjyOr4-nLCvXVVQSDL7rD7iLRb6
12    JmBcCzyfDuKgFNW0gOaPmYb0XbFR_pwZulKUYs94eZoa0K3TV9gPTwIqWUi-mbZ9D2YS2uoPraL7lwxI6MKmgdL3DmM
13    C083Wgsq8IkuEiKa-eGZjpJHAXdcIs3NqCJ5j2ua77RbHB4kXbkZyM8xPk7K_OW0zRNGsH-BNLD90XKE_Qx6A_oJzL9
14    hAW2RIqGAHBEO-0wp5AReVgIODhIyMkEWX8Hai14XOTid8</tkDesafio>
15   </retRegistro>
16 </iniciarRegistroResponse>
```

B.1.3 Mensagem DAF registrar

B.1.3.1 Pedido - mensagem 6

Listagem B.6: Documento JSON para o pedido da mensagem registrar

```
1 {
2   "msg": 1,
3   "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJubmMiOiJzbnZoZ1h0Zno2SDgwSDlsQk50NGtnIn0.
4     TJg17N31-6K0xizFe81o0dGEKQzIft3BSRGoFbWE7QQeBEHdbvbZ57ik4HjLpBytSyBqpjouukXfbizSEaAMZUBA
5     pftXBfBjUL5RzQH66n9r0x08QCYWECG-12Pri9j2b7k5FbjinLSNia0sTaDk0EcNSi2muJsH6131IY4sXDJQcNNC
6     AkaunSpAz5SjUstfnuCFKriK9jNOjWQTGntQRC_A6cY_A1FrLxinLpl-b0fuNLk06INvutKgEqen-LCrWRM8CZav
7     a0VqLFAaitJgvDic0qITqHd-iZg97IPp3PdjofOKAk0ci_gIEryHx31U_j9i1U9Tjp31D-nm4ISSKh3jHx5KrRvG
```

```

Ddw09rzprrzmLapc-Ub8QJtgxVgcr-__NHvg_9RfT1CEwGeOELRNsLW-HsOp03kHc_-yXnmm0oD-Gjy0r4-nLCvX
VVQSDL7rD7iLRb6JmBcCzyfDuKgFNW0g0aPmYbOXbFR_pwZulKUYs94eZoaOK3TV9gPTwIqWUi-mbZ9D2YS2uoPr
aL7lwxI6MKmgdL3DmMCO83Wgsq8IkuEiKa-eGZjpJHAXdcIs3NqcJ5j2ua77RbHB4kXbkZyM8xPk7K_0W0zRNGsH-
BNLD90XKE_Qx6A_oJzL9hAW2RIqGAHBE0-0wp5AReVgI0DhIyMkEWX8Hai14X0Tid8
4 }

```

B.1.3.2 Resposta - mensagem 8

A resposta do DAF para a mensagem recebida é um aninhamento de dois *tokens* JWT. Desta forma, a Listagem B.7 apresenta o cabeçalho e o conteúdo (veja Tabela 6.4) para a geração do primeiro *token* JWT, assinado com a chave privada do DAF (chave RSA).

Listagem B.7: Cabeçalho e conteúdo do *token* JWT a ser assinado com a chave privada do DAF

```

1 {
2   "typ": "JWT",
3   "alg": "RS256",
4   "jwk": {
5     "kty": "RSA",
6     "n": "iizMtgRaFIqua_wTlSfQWCERWEDFhBJQ-H6FDtnE8sQ5uIeFDfNmT_BuBihcCD72gsCAdSWspXiFzNyn1jME
       gysBBpC5u2lzzhZkR-oKMH6RacS1puQ_LLmdF3Kq6nbMZptF66yND01GYU-cUqWH2A5f3X6kjjGi8YNr1Vis6k-wL8
       ta1qLM4ZFpZgWHWCgjeM-k0Tg3qZbzylamsHFxQgUXb4Ab06fjSvyVZri1opxU_mam0fWGcgTQcZ2qoppAXGOZf50P
       n6_3zA0wX8gWVU93rCg5GPXj-u7XTAVN-QQiFzveso_EPPTWG1HgSF3nNy4L08xHVPdL5srLr1M6Fw",
7     "e": "AQAB"
8   }
9 }
10 {
11   "daf": "YRaQYtWtROCSI-gCuL7oyg",
12   "cnt": 0,
13   "nnc": "snvhgXNfz6H80H91BNt4kg"
14 }

```

A Listagem B.8 apresenta o cabeçalho e o conteúdo para a geração do segundo *token* JWT, dessa vez assinado com a chave de ateste (chave RSA). O conteúdo deste *token* JWT é o *token* JWT gerado a partir da Listagem B.7.

Listagem B.8: Cabeçalho e conteúdo do *token* JWT a ser assinado com a chave de ateste

```

1 {
2   "typ": "JWT",
3   "alg": "RS256",
4   "jwk": {
5     "kty": "RSA",
6     "n": "7uPdSsasBsc1bkHrciKXue4fftAJvkCi66pMpMqebSfv808in2ZWtgICFBn4tTLp6UXCin2-RigqS_SM8I455
       ZQDEVgwuKsvojuUUTE1ljcyoqH4yeqvIeRnKkq1N11bH4C6S9AGpPHSItNeusAYtvaAjCSY8HvB3xTm2L3ufziw5U3W
       nxfoAsYUKhvD1T1_Hy47vhWlfdxvdLnc0qD5Cdb-FRnUJJ8pV5yNpyNpjLo_78XTjFuoShct382MjCCKPA7c7JhOMHT
       Vs0dyfe19c3JaTqalsgAiFNB2Cg_ZtvCQ9KQkv3XBz1b2ShE5fY--Y9vGeQbTdkDxK0PqoEy0jSTEEgHJqHYyp804i
       uAe-7ia_gC7BxBQVfUHwaXIZmPPQMs83HSaRPQF3L_r2_a134u0LIgnSTL0oTvuI4igYPQLy7Xme-afF5roxct6jdw8
       BhgHwYvZ1FJDNKJ3hX8YYbv5qc3iORAFiiK5B1L9SN0fDSd7tXCIBieB3zZjG0-Z6ZI3KzEiKLRG4WPp3WTBxX3Ybi
       ebP7V-SWORuQJmgxcqxw01qzvZQuCg9oSMQ7DOW2yPTrZa4t2fJNCL9gQ4xuQ8aHlklRtsK8Uu0NmVg78ugakN1OAZ
       r074uzJUKWBwz3PKjz9K6f_QEi3S87SbTZ0qmCNmkceZk6Tnld-8",
7     "e": "AQAB"
8   }
9 }
10 {
11   "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp3ayI6eyJuIjoiaW16TXRnUmFGSXF1YV93VGxzZ1FXQ0VS
       VOVERmhCS1EtSDZGRFRuRThzUTV1SWVGRGZ0bVRFQnVCAWhjQ0Q3MmdzQ0FkU1dzcFhpRnpOeW4xak1FZ3lzQkJwQz
       V1Mmx6emhaa1Itb0tNSDZSYWNTMxB1UV9MTG1krjNlcTzUyK1acHRGNjZ5TkrPbEdZVS1jVXFSDJBNWYzWDZrampH
       aThZTnIxVmlzNmstd0w4dGExcUxNNFpGcFpnd0hXQ0dqZU0ta09UZzNxWmJ6eWxhbXNIRnRZ1VYYjRBYjA2ZmpTdn
       lWw1JpMW9weFVfbWfMGZXR2NnVFFjWjJxb3BwQVhHT1pmNU9QbjZfM3pBT3dYOGdXV1U5M3JDZzVHUFhQLXU3WFRB
       Vk4tUVFpRnp2ZXNvXOVQURXRzFIZ1NGM250eTRMMDh4SFZQZEw1c3JMcmxNNkZ3IiwiZSI6IkFRQUiLiCJrdHkiOi
       JSU0EifX0.eyJkYXYiOiJZUmFRWXRxdFJPQ1NjLWdDdUw3b3lnIiwiaWY250IjowLCJubmMiOiJzbnZoZ1h0Zno2SDgw
       SDlsQk50NGtnIn0.hhbV04DpboXY2jE8AvH2iEs_cgXrWc9f-WDpZaaAacQqat7ZMLZiIm-vhJvQ0y-XHZMqElz2C0
       bXXCHWeSU3e18PqxqNwMcy5WhqJhPoCOI3Jh8mtgonIpDBtY6Cr_oTnytNpSMXwQD80n85rTC4YjvqyyZfdLztzZpu
       irD31kiS4sX_mj8bjZcOyVubxTX6SBYBpIWsC5AvGDmhlQ2rh9rVILxVwpWJWDBwXMsE7U4pQpx6f-lzzC99zkvAu
       11Hjywyb2n50MGspPOTVcp_wPUJLEAKtd3Sk_eLhF-I4MdWjyEVxgQKG10GbBSRoRmdwHEWjNdhaeaQnfs4fv17g"
12 }

```

Por fim, a Listagem B.9 apresenta a resposta do DAF para a mensagem recebida, que carrega o *token* JWT gerado a partir da Listagem B.8 .

Listagem B.9: Documento JSON para a resposta da mensagem registrar

```

1 {
2   "res": 0,
3   "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp3ayI6eyJuIjoiaW16TXRnUmFGSXF1YV93VGxzZ1FXQ0VS
       nRBSnZrQ2k2NnBNcE1xZWJtZnY4TzhpbjJaV3RnSUNGQm40dFRMcDZVWENpbjItUmlncVNfU004STQ1NVpRREWVZ3d1
       S3N2b2pVVVVURWxsamN5b3F1NH1lcXZJZVJuS2txbe4xMWJINEM2Uz1BR3BQSFNpdE5ldXNBWXR2YUFqQ1NZ0Eh2Qj
       N4VG0yTDN1ZnppdzVVM1dueGZvQXNZVUtodkRsVDFfSHk0N3oV2xmRHh2ZEeX0Y09xRDVDZGItr1JuVUpKOHBNX10
       cH10cGpMb1830FhUakZ1b1NoY3QzODJNakNa1BBN2M3SmgwTUuVnNPZHlMzTE5YzNKYVVRxYwXzZ0FpRk5CMkNnX1
       p0dkNR0UtRS3ZRM1hCeJFiMlNoRtVmWS0tWT12R2VRY1RkS0R4SzbQcW9FeTBqU1RFRWdISnFIWVlwOE80aXVBZS03
       aWFFzOM3QnhCUVZmVUHXYVhJWm1QUFFNczgzSFNhu1BRrjNMx3IyX2EXmzR1MEXJZ25TVEwbb1R2dUk0aWdZUFFMeT
       dYbWUtYWZGNXJveGNONmpkVzhCaGdId112WjFGSkROS0ozaFg4WV1idjVxYzNpMFJBRmlpaUs1Qkls0VNOMGZEU2Q3
       dFhDSUJpZUizelpqRzAtWjZaSTNLeKvPS0xyRzRXUHAzV1RCeFgzWWJpZWJQN1YtU1cwUnFVSM1neGNxeHcwMXF6d1
       pRdWNH0W9TTE3RDBXmnlQVHJaYTROMmZKtkNMOWdrNhh1UThhSGxrTFJ0c0s4VXUwTk12Rzc4dWdha05sMEFack83
       NHV6S1VLV0J3ek0zUeTqeJlLnMzUUVpM1M4N1NiVfowcW1DTm1rY2VaazZUbmXkLTgiLCJlIjoieQVFBQiIsImt0eS
       I6I1JtQSJ9fQ.eyJkd3QiOiJleUowZVhBaU9pSktWMVFPtENKaGJHY21PaUpTVXpJMU5pSXNjYXZlYX1JNmV5SvVJa
       m9pYVdsNlRYUm5vUZHU1hGMVlWOTNWR3h6WmxGWFewV1NWMFZFUm1oQ1NsRXRTRFpHUkZSdVJUaHpvVfYxU1dWR1J
       HwK9iV1JmUW5WQ2FXaGpRMFEzTW1ke1EwRmtVMWR6Y0zocFJucE91VzR4YwsxRl0zbHpa0p3UXpWmu1teDZ1bWhhY
       TFJdGIdE5TRFpTWVd0VE1YQjFVVjlNVEcxa1JqTkkjVfP1WwsxYWNiUkd0a1o1VGtSUGJFZFpWUzFqVlhGWFNESKJ
       OV116V0RacmFtcEhhVGhaVG5JeFzTbHp0bXN0ZDB3NGRHRXhjVXh0TkZwR2NGcG5kMGhYUTBkcVpVMHRhMD1VWnp0e

```



```

MwtpUzRzWF9tajhialpjT3lWdWJ4Vfg2U0JZQnBJV3NDNUF2R0RtaExRMnJo0XJWSUx4VndwVOpXVORCd3hNc0U3VTR
wUXB4NmYtbHp6Qzk5emt2QXVsMUhqeXdieTJuNU9NR3NwUE9UVkNwX3dQVUpMRUFLdGQzU2tfZUxoRi1JNE1kV2p5RV
Z4Z1FLR2xPR2JCU1JvUm1kd0hFd2pOZGhhZWRfBmZzNGZwbDdnIn0.6Khc9wdxMq_OKBRV0JOXoSAM0g9Q5Y8Ixghgj
M_G3y6V7dnfLqW05k1shBDLjNG3xJd9q9hHlJcFNdsTqXcb-OZujSFZITW_YbhKJcbYOIRCrBxb1bkn7Nplpr07WgFP
luFWLGXIEyWReWfe4TsPCkfxWJZ-Wf0VTLJuEzxxkysJ1_VoCfOhsUaBTF0tri3kE_Gwq1RB3zYh_W736U5_onE3REZ
qnItlFH5DhSouznPvGIOHLWo9QAaha9irg_BD1MMTrHjND8zFBpm0-GGmaCB01V7aJaNjtZV4ai3UM1Yb4mxi50JFMg
lQ_s0g7F3cHdgzGt4KwOU-z6u_myh-mzHZm0k00E7Vb3dVU98qy0gJyJtztjl6GbnCTc_5hRbtuhmWPLrp3zsYz8wAu5
YSEZQLGPQzqyLNZ8N0_Fi2gJdQKAskKrwlaT3Gni4pW8tX5d2kKp04pw9cimSK_M9TA1Q0BLd9miH3GtieOst1svfTt
x_Z-Ez1lwHW6Ggp2fEPA7ROT3s1PvflAfma9I3mTF32CshDtj_ao7p9VNNrt_Uh_7_1eZAmJimh8UEE0uYhd68KRNZ
Uv5wfBQ8fVFT-3Ws_xlhb1hHK5P_KYr4F0usWmkepIiYcqtJKWs9LRvWbnw7Wg8gJx4TwV-rxX0eNzuaKayh8eXntou9
we-1iDE</tkAut>
7 </infConfRegistro>
8 <Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><!--Assinatura--></Signature>
9 </pedConfRegistro>
10 </confirmarRegistro>

```

B.1.4.2 Retorno - mensagem 11

A SEF irá gerar um *token* JWT que deverá ser incorporado no documento XML do retorno. A Listagem B.11 apresenta o cabeçalho e o conteúdo (veja Tabela 6.5) para a geração do *token* JWT. Neste exemplo, o *token* JWT é assinado com a chave privada da SEF (chave RSA) par da chave pública contida no certificado digital da SEF que está presente no DAF. O retorno da SEF é apresentado na Listagem B.12 e o *token* JWT gerado a partir da Listagem B.11 pode ser encontrado dentro do campo tkChaves.

Listagem B.11: Cabeçalho e conteúdo do *token* JWT que será incorporado no retorno do método confirmarRegistro

```

1 {
2   "typ": "JWT",
3   "alg": "RS256"
4 }
5 {
6   "chs": "AcqkAZ6bpF6lagBqq0lshI_kTXx1BwLnJpdag2yYlQugLmOMiWulPVNXuHXfYWhwaw2XmyZc7cyvrn66B67
DYWOXWKOAb-kxsoHtkxL0LgqYo0pW02j2ZcN90dYbKacxzicTucpdCve5w63gvHNuRBM_blmi3Z1ETF5Hm5H2J1A01N
fUReKxG1E5cGmbGqWbs4vF14NOUT-I7rfMMcAGswYF0twrZ0JEpjRq6cGTs5qeQm9YRj_X_GnQqWAjsypVnCOneKvKZ
Eq12Wuo6rPw-vcv-FY0uG-mcZn5qe1rTcwM46Kd8j5kGsq4M1-L5Scxhywro6Gap40tMz6EAk6GoA",
7   "chp": "PVGhC0gSqrzx0q1nosnX3e4Th0ycNFwg1nV1l-Pxw1TpgnUjCyCg476f9A1_-7WZxLq1XzP6L3_vmFgYR8rw",
8   "mop": 0
9 }

```

Listagem B.12: Documento XML de retorno do método confirmarRegistro

```

1 <confirmarRegistroResponse xmlns="http://www.portalfiscal.inf.br/daf/wsd/DAFRegistroDispositivo">
2   <retConfRegistro versao="1.00" xmlns="http://www.portalfiscal.inf.br/daf">
3     <idDAF>YRaQYtWtROCSI-gCuL7oyg</idDAF>
4     <cStat>1001</cStat>
5     <xMotivo>Dispositivo registrado com sucesso</xMotivo>
6     <tkChaves>eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJjaHMiOiJBYS3FrQVo2YnBGNmxhZ0JxcU9sc2hJX2t
UWHgxQndMbkwZGFmMn1ZbFF1Z0xtT01pV3VsUFZOWHVlWGZZV2h3YXcyWG15WmM3Y312cm42NkI2NORZVzBYV0tPQ
WIta3hzb0h0a3hMMEexcV1vMHBXMDJqM1pjTjkwZFl1S2FjeHppY1R1Y3BkQ1Z1NXc2M2d2SE51UkJNX2JsbWkzWjF
FVEY1SG01SDJKMUEwE5mVVJlS3hHMUU1Y0dtYkdRd2JzNHZGMTR0T1VULUk3cmZNTWNBR3N3WUYwdHdyWjBKRXBqU

```

```

nE2Y0dUczVxZVFt0V1Sa19YX0duUXFXQWpzeXBWbkNPbmVLVmtaRxFsM1d1bzZyUHctdmN2LUZZMHVHLW1jWm41cWV
sclRjd000Nktk0Go1a0dzcTRNbC1MNVNjeGh5d3JvNkdhcDQwdE16NkVBazZHb0EiLCJjaHAi0iJQVkdQzBnR3Nxc
np4MHExbm9zblgzZTRUaE95Y05GV2cxb1ZJbC1QeFdsVHBnb1VqQ31DZzQ3NmY5QWxfLTdXWnhMcWxYWnBYNkwzX3Z
tRmdZUjhydyIsIm1vcCI6MH0.MAdeB4qqJ4rfghkyB255W64GddK_b0BAUoF125xenHI-kTD4o02bZcyfjPsPXJewt-
RIk9-VdWEmTnKw0Qr8T_o-ouVhZgeOHDg3WcHo88ezenP3ekSp5QkASTuCaN2EKN3m--hTArqhcYnyx0nX2dreqZUb
TyWbA3HJdrkxq3W9AiK0ZG-fyugUcRD1GpHEhX2WwRj9j66tGxaU3jEt_PZJmVg6dqnVhcjvEW7vpPvFdon8DfG87l
uMnwoWoL2HjyDOfldL1hU56-AQAr3oZBVNmzf_Hvi8dF9bUPdtetozhTCdFw79WxhWlc_DqDCNLgv0VU46hvaGI8p02
sB5y4Kbb56g0MsZU_ZeY6A4W533m9Y-S0k9SyDQLSqMBCG-WAprNd1vDVGXRfiZL2Z9GESyg5Yq7rFaQDpPCM7hjPe
TW5dCDsa0q-VC89p8-qDC61qDD4PmXfKB7-mqsDsDJPu30FQQ8hJvhvWRI9d2fd5hEmGvhmelhvLUwmCT0hL9-LtMa0
xxfPQrV3o9vSLjNUJFga04aLdTvwlgZ4rVzA2Jqqp9WVihII-cfa-gbM-w60QdqtI0mSNWJMsEBxWt1Pt3bxwkqEDU
j0ncrJNQoMsU9daH0B8A_8LXEyoXec80yx_oMFvVQBsmYoe1Fljf-pp0c4rdqKtZQYBpX5BWP6g</tkChaves>
7 </retConfRegistro>
8 </confirmarRegistroResponse>

```

B.1.5 Mensagem DAF confirmarRegistro

B.1.5.1 Pedido - mensagem 12

Listagem B.13: Documento JSON para o pedido da mensagem confirmarRegistro

```

1 {
2   "msg": 2,
3   "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJjaHMiOiJBY3FrQVo2YnBGNmXhZ0JxcU9sc2hJX2tUWH
  gxQndMbkpwZGFnMnlZbFF1Z0xtT01pV3VsUFZOWHVIWGZZV2h3YXcyWG15WmM3Y312cm42NkI2NORZVzBYV0tPQWIta3
  hzb0h0a3hMMEexcVlVMBXMDJqM1pjTjkwZFliS2FjeHppY1R1Y3BkQ1Z1NXc2M2d2SE51UkJNX2JsbWkzWjFFVEY1S
  G01SDJKMUEwbE5mVWJlS3hHMU1Y0dtYkdRd2JzNHZGMTR0T1VULUk3cmZNTWNBR3N3WUYwdHdyWjBKRXBqUnE2Y0dU
  czVxZVFt0V1Sa19YX0duUXFXQWpzeXBWbkNPbmVLVmtaRxFsM1d1bzZyUHctdmN2LUZZMHVHLW1jWm41cWVsc1Rjd000
  Nktk0Go1a0dzcTRNbC1MNVNjeGh5d3JvNkdhcDQwdE16NkVBazZHb0EiLCJjaHAiOiJQVkdQzBnR3Nxcnp4MHExbm9
  zblgzZTRUaE95Y05GV2cxb1ZJbC1QeFdsVHBnb1VqQ31DZzQ3NmY5QWxfLTdXWnhMcWxYWnBYNkwzX3ZtRmdZUjhydy
  IsIm1vcCI6MH0.MAdeB4qqJ4rfghkyB255W64GddK_b0BAUoF125xenHI-kTD4o02bZcyfjPsPXJewt-RIk9-VdWEmT
  nKw0Qr8T_o-ouVhZgeOHDg3WcHo88ezenP3ekSp5QkASTuCaN2EKN3m--hTArqhcYnyx0nX2dreqZUbTyWbA3HJdrkx
  q3W9AiK0ZG-fyugUcRD1GpHEhX2WwRj9j66tGxaU3jEt_PZJmVg6dqnVhcjvEW7vpPvFdon8DfG87luMnwoWoL2HjyD
  OfldL1hU56-AQAr3oZBVNmzf_Hvi8dF9bUPdtetozhTCdFw79WxhWlc_DqDCNLgv0VU46hvaGI8p02sB5y4Kbb56g0M
  szU_ZeY6A4W533m9Y-S0k9SyDQLSqMBCG-WAprNd1vDVGXRfiZL2Z9GESyg5Yq7rFaQDpPCM7hjPeTW5dCDsa0q-VC89
  p8-qDC61qDD4PmXfKB7-mqsDsDJPu30FQQ8hJvhvWRI9d2fd5hEmGvhmelhvLUwmCT0hL9-LtMa0xxfPQrV3o9vSLjN
  UJFga04aLdTvwlgZ4rVzA2Jqqp9WVihII-cfa-gbM-w60QdqtI0mSNWJMsEBxWt1Pt3bxwkqEDUj0ncrJNQoMsU9daH0
  B8A_8LXEyoXec80yx_oMFvVQBsmYoe1Fljf-pp0c4rdqKtZQYBpX5BWP6g
4 }

```

B.1.5.2 Resposta - mensagem 14

Listagem B.14: Documento JSON para a resposta da mensagem confirmarRegistro

```

1 {
2   "res": 0
3 }

```

B.2 Remover registro do DAF junto à SEF

Os exemplos apresentados referem-se as mensagens ilustradas no diagrama de sequência apresentado na Figura 5.8. O processo operacional é detalhado na Seção 5.5 e fluxos alternativos e de exceção para esse processo são apresentados nos Casos de Uso UC-4.11 e UC-4.2.

B.2.1 Serviço SEF DAFRemocaoRegistro - método removerRegistro

B.2.1.1 Entrada - mensagem 2

Listagem B.15: Documento XML de entrada do método removerRegistro

```
1 <removerRegistro xmlns="http://www.portalfiscal.inf.br/daf/wsd/DAFRemocaoRegistro">
2   <pedRemRegistro versao="1.00" xmlns="http://www.portalfiscal.inf.br/daf">
3     <infRemRegistro Id="DAFYRaQYtWtROCSI-gCuL7oyg">
4       <idDAF>YRaQYtWtROCSI-gCuL7oyg</idDAF>
5       <idPAF>3BV9hxwDwDkzQf2R6hEqHfNevwsuRtVvEHfJto9N0qE</idPAF>
6       <xJust>Justificativa para remover registro DAF.</xJust>
7     </infRemRegistro>
8     <Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><!-- Assinatura --></Signature>
9   </pedRemRegistro>
10 </removerRegistro>
```

B.2.1.2 Retorno - mensagem 3

A SEF irá gerar um *token* JWT que deverá ser incorporado no documento XML do retorno. A Listagem B.16 apresenta o cabeçalho e o conteúdo (veja Tabela 6.10) para a geração do *token* JWT. Neste exemplo, o *token* JWT é assinado com a chave privada da SEF (chave RSA) par da chave pública contida no certificado digital da SEF que está presente no DAF. O retorno da SEF é apresentado na Listagem B.17 e o *token* JWT gerado a partir da Listagem B.16 pode ser encontrado dentro do campo tkDesafio.

Listagem B.16: Cabeçalho e conteúdo do *token* JWT que será incorporado no retorno do método removerRegistro

```
1 {
2   "typ": "JWT",
3   "alg": "RS256"
4 }
5 {
6   "nnc": "wuOPSi-BwqdVfibFk0-oQg"
7 }
```

Listagem B.17: Documento XML de retorno do método removerRegistro

```
1 <removerRegistroResponse xmlns="http://www.portalfiscal.inf.br/daf/wsd/DAFRemocaoRegistro">
2   <retRemRegistro versao="1.00" xmlns="http://www.portalfiscal.inf.br/daf">
3     <idDAF>YRaQYtWtROCSI-gCuL7oyg</idDAF>
4     <cStat>1000</cStat>
5     <xMotivo>Solicitação recebida com sucesso</xMotivo>
6     <tkDesafio>eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJubmMiOiJ3dU9QU2ktQndxZFZmaWJGa08tb1FnIn0.
7     BUCSa6xRN11g_7Ls-MDg9Zq66gJRWcVkvHVhsS3Yc-v6e-LIKJxzfQ2u2VsjrAowXdQtSrV3boTTT4VjUoSBvWtwUWZ
8     _vwlSiSUDXo1ZrVgTHT05PcCfndV-T0tfsgCC1CPLQFTLhtCn6PJutisWyftg18eIk0gVwPGJtTBS41acJTgv6Rx3YU
9     HG8tmLAajP14Eg5x4XMd0Saj0thdpZFSSn2BFYJhCeRzUfgopJolMeTwJE9o3wX9ytEMjp3e6_Qzt58qBN1vpSCMG5o
10    ZNZLVse22YchqrpTBBfHYkfHjMStIQPNAI6x0pAtB50iTCgSJVkr5mx3_L_DkhqeAUDq81XmuXpgf8DdgAZERy2_AXIS
11    MsKhewHw5-5zWPqwx5-adtVfpfwa6WkwCIYF8qgRIHv6jYGmfccLfuh1Sd7s9-nYLOYfQ_Qv3kEKVgybY4-iF-DoN2
12    fseeVt_Hex6q8IiMyC7NgAujcBKdeVZk0g5A1VTexm3YPHquHkp9eIgnDbef6woeGucj2rU0hC11tOraIP-q_J5WczF
13    HUHCbBDN0bK9xrTLfY5BGwdBQFU5_ks-ewXHqYr0lg0IEBz9gjj6AskfxhiyHq0TNTZw8P8_tjyTZx3J7B1-rVpFYhb
14    muU-PXLE_Yyz7HDQnX4sMW1VLJCOjYGw1FzdEzz-usUDaM</tkDesafio>
```

```
7 </retRemRegistro>
8 </removerRegistroResponse>
```

B.2.2 Mensagem DAF removerRegistro

B.2.2.1 Pedido - mensagem 4

Listagem B.18: Documento JSON para o pedido da mensagem removerRegistro

```
1 {
2   "msg": 6,
3   "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJubmMiOiJ3dU9QU2ktQndxZFZmaWJGa08tb1FnIn0.
   BUCSa6xRN11g_7Ls-MDg9Zq66gJRWcVkvHVhsS3Yc-v6e-LIKJxzfQ2u2VSjrAowXdtSrV3boTTT4VjUoSBvWt
   wUWz_vwlSiSUDXo1ZrVgTHT05PcCfndV-T0tfsgCC1CPLQFTLhtCn6PJutisWyftg18eIk0gVwPGJtTbs41acJT
   gv6Rr3YUHG8tmLaajP14Eg5x4Xmd0Saj0thdpZfSSn2BFYJhCeRzUfgopJolMeTwe9o3wX9ytEMjp3e6_Qzt58
   qBN1vpSCMG5oZNZLVse22YchqrpTBBfHYkfHjMStIQPNAI6x0pAtB50iTCgSJVkr5mx3_L_DkhqeAUDq81XmuXp
   gf8DdgAZERy2_AXSMskhewHw5-5zWPqwx5-adtVpfwa6WkwCIYF8qgRIHv6jYGmfccLfuhlSd7s9-nYLOYfQ_
   Qv3kEKVgybY4-iF-DoN2fseeVt_Hex6q8iMyC7NgAUjCBKdeVZk0g5A1VTextm3YPHquHkp9eIgnDbef6woeGuc
   j2rU0hC11t0raIP-q_J5WczFHUHCBDN0bK9xrTLfY5BGwdBQFU5_ks-ewXHqyr0lg0IEBz9gjj6AskfxhiyHq0
   TNTZw8P8_tjyTZx3J7B1-rVpFYhbmU-PXLE_Yyz7HDQnX4sMW1VLJC0jYGw1FzdEzz-usUDaM"
4 }
```

B.2.2.2 Resposta - mensagem 6

O DAF irá gerar um *token* JWT que deverá ser incorporado na resposta da mensagem. A Listagem B.19 apresenta o cabeçalho e o conteúdo (veja Tabela 6.11) para a geração do *token* JWT. Neste exemplo, o *token* JWT é assinado com a chave privada do DAF (chave RSA). A resposta da mensagem é apresentada na Listagem B.20.

Listagem B.19: Cabeçalho e conteúdo do *token* JWT que será incorporado na resposta da mensagem removerRegistro

```
1 {
2   "typ": "JWT",
3   "alg": "RS256"
4 }
5 {
6   "daf": "YRaQYtWtROCSI-gCuL7oyg",
7   "cnt": 1,
8   "nnc": "wuOPSi-BwqdVfibFk0-oQg"
9 }
```

Listagem B.20: Documento JSON para a resposta da mensagem removerRegistro

```
1 {
2   "res": 0,
3   "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJkYWkiOiJ3dU9QU2ktQndxZFZmaWJGa08tb1FnIn0.F2FI1pNy8QcY0KqL0gLRudULP5wXCV3vXccfRS-M
   rd52m66Qg42AmFYko8w4X-ZkaiYrCbZNG8b9egRR0aB6oHv9r74-tVD6JK68KRYAwfASaTKMk0258eWkDR8T-g5-gz-
   bxcoF_XCRtWLO1zV3ejm32m2OFFjB8QVgiWsjWSKn4Tcg5vuc4g2TwbBBFLeLE6CNbn3CGmr0epdNzU0pAoERhvqh
   EZaCNfqe8jheb-s7rrH1vtwFOYfa3JpW-oR0kUCfoK6G6tfsDgxVDbyk4_yg3IuOD_CgpGVnC27ErHv1cJh67Vip8y
   C30Q69br6Zj1vHdFz98rdMp41-75w"
```

```
4 }
```

B.2.3 Serviço SEF DAFRemocaoRegistro - método confirmarRemoveRegistro

B.2.3.1 Entrada - mensagem 7

Listagem B.21: Documento XML de entrada do método confirmarRemoveRegistro

```
1 <confirmarRemoveRegistro xmlns="http://www.portalfiscal.inf.br/daf/wsd/DAFRemocaoRegistro">
2   <pedConfRemRegistro versao="1.00" xmlns="http://www.portalfiscal.inf.br/daf">
3     <infConfRemRegistro Id="DAFYRaQYtWtROCSI-gCuL7oyg">
4       <idDAF>YRaQYtWtROCSI-gCuL7oyg</idDAF>
5       <idPAF>3BV9hxwDWDkzQf2R6hEqHfNevwsuRtVWEHfJto9N0qE</idPAF>
6       <tkAut>eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJkYXV0eXkiOiJZUmFRWXRXdFJPQ1NjLWdDdUw3b3lnIiwia250IjoxcjJubmMiOiJ3dU9QU2ktQndxZFZmaWJGa08tb1FnIn0.F2FI1pNy8QcYOKqLQgLRudULpF5
7       wXCV3vXccfRS-Mrd52m66Qg42AmFYko8w4X-ZkaiYrCbZNG8b9egRR0aB6oHv9r74-tVD6JK68KRYAwfASaT
8       KMk0258eWkDR8T-g5-gz-bxfcoF_XCRtWLOlZV3ejm32m20FFjB8QVgiWsjWSKn4Tcg5vuc4g2TwbBBFLeLE6
9       CNBn3CGmrOepdNzU0pAoERhvqhEzACnfqe8jheb-s7rrH1vtwFOYfa3JpW-or0kUCfoK6G6tfSdgxVDbyk4_
10      yg3IuOD_CgpGVnC27ErHv1cJh67Vip8yC30Q69br6Zj1vHdFz98rdMp41-75w</tkAut>
11     </infConfRemRegistro>
12     <Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><!-- Assinatura --></Signature>
13   </pedConfRemRegistro>
14 </confirmarRemoveRegistro>
```

B.2.3.2 Retorno - mensagem 8

A SEF irá gerar um *token* JWT que deverá ser incorporado no documento XML do retorno. A Listagem B.22 apresenta o cabeçalho e o conteúdo (veja Tabela 6.12) para a geração do *token* JWT. Neste exemplo, o *token* JWT é assinado com a chave privada da SEF (chave RSA) par da chave pública contida no certificado digital da SEF que está presente no DAF. O retorno da SEF é apresentado na Listagem B.23 e o *token* JWT gerado a partir da Listagem B.22 pode ser encontrado dentro do campo *tkEvento*.

Listagem B.22: Cabeçalho e conteúdo do *token* JWT que será incorporado no retorno do método confirmarRemoveRegistro

```
1 {
2   "typ": "JWT",
3   "alg": "RS256"
4 }
5 {
6   "evn": "REMOVED"
7 }
```

Listagem B.23: Documento XML de retorno do método confirmarRemoveRegistro

```
1 <confirmarRemoveRegistroResponse xmlns="http://www.portalfiscal.inf.br/daf/wsd/
2   DAFRemocaoRegistro">
3   <retConfRemRegistro versao="1.00" xmlns="http://www.portalfiscal.inf.br/daf">
4     <idDAF>YRaQYtWtROCSI-gCuL7oyg</idDAF>
5     <cStat>1002</cStat>
```

```

5 <xMotivo>Registro de dispositivo removido</xMotivo>
6 <tkEvento>eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJldm4iOiJSRU1PVkVSIn0.AyYUS84vVEhIi8ywPAROZ
  a2QSPs7LywHFbkn_S2_4Pee7wvyGgBekuu0dqykSOo8vdruYQkjLZtSOKOf9d0-rFL7SetBxcGW355ppCret0gDwTKS
  BhdN1s0aGqDdNHLILk65oXI6_g-foSGYYqhVgS-WqTdPAV5hloQSAtdDSTBto2f0f0EcEx0Xpla5_8RIEzgvCT91CL-U
  lLeecYNor7deevuwtfqePUFoLilvKCLoahpR5_hLc2ijk0taDvvuH4aRSNGiLi5SEuK6FI_BtLqatRw1Qu0e0WizIE3n
  dY09q77q55EtCTzDY9ogf_FfgIwblZc8Ne77iWaJNoxQyDvK26ewTn7Ac3I4oTmBEnaGX8M4GC_3Mpi0EqVkJRWZlhc7
  TlXrjLXacnS004gLhppTWdVd62sADbENXqVaXoVx75-WhM04-t_1LsMCTUUtqWlwnFPLPn4dwrGj8xZdZgEXPWj7DLzo
  zr7smZ0m3E7tJ3CHCq7-_03151X0vxDBF0tC3USFrT77iSRzCPZhsqfEINwVRSzhQ_xVdLfjbrmzrSnpQNu36FK8Jgch
  MvLXbT-oOn_U1C4P5qbpjWsuE6AY880a_E4CSZK3tEnCaTTHEMbpOrN0hap0tzUxteBYoe9N0w3rKHwnYcmUHxIVC_YM
  idBnKF-YW9i_FH6zKw</tkEvento>
7 </retConfRemRegistro>
8 </confirmarRemoverRegistroResponse>

```

B.2.4 Mensagem DAF confirmarRemocaoRegistro

B.2.4.1 Pedido - mensagem 9

Listagem B.24: Documento JSON para o pedido da mensagem confirmarRemocaoRegistro

```

1 {
2   "msg": 7,
3   "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJldm4iOiJSRU1PVkVSIn0.AyYUS84vVEhIi8ywPAR
  OZa2QSPs7LywHFbkn_S2_4Pee7wvyGgBekuu0dqykSOo8vdruYQkjLZtSOKOf9d0-rFL7SetBxcGW355ppCr
  et0gDwTKSBhdN1s0aGqDdNHLILk65oXI6_g-foSGYYqhVgS-WqTdPAV5hloQSAtdDSTBto2f0f0EcEx0Xpla5
  _8RIEzgvCT91CL-UlLeecYNor7deevuwtfqePUFoLilvKCLoahpR5_hLc2ijk0taDvvuH4aRSNGiLi5SEuK6F
  I_BtLqatRw1Qu0e0WizIE3ndY09q77q55EtCTzDY9ogf_FfgIwblZc8Ne77iWaJNoxQyDvK26ewTn7Ac3I4oT
  mBEnaGX8M4GC_3Mpi0EqVkJRWZlhc7TlXrjLXacnS004gLhppTWdVd62sADbENXqVaXoVx75-WhM04-t_1LsM
  CTUUtqWlwnFPLPn4dwrGj8xZdZgEXPWj7DLzozr7smZ0m3E7tJ3CHCq7-_03151X0vxDBF0tC3USFrT77iSRz
  CPZhsqfEINwVRSzhQ_xVdLfjbrmzrSnpQNu36FK8JgchMvLXbT-oOn_U1C4P5qbpjWsuE6AY880a_E4CSZK3t
  EnCaTTHEMbpOrN0hap0tzUxteBYoe9N0w3rKHwnYcmUHxIVC_YMidBnKF-YW9i_FH6zKw"
4 }

```

B.2.4.2 Resposta - mensagem 11

Listagem B.25: Documento JSON para a resposta da mensagem confirmarRemocaoRegistro

```

1 {
2   "res": 0
3 }

```

B.3 Autorização de Documentos Fiscais Eletrônicos (DF-e)

Os exemplos apresentados referem-se as mensagens ilustradas no diagrama de sequência apresentado na [Figura 5.3](#). O processo operacional é detalhado na [Seção 5.2](#) e fluxos alternativos e de exceção para esse processo são apresentados nos Casos de Uso [UC-4.6](#), [UC-4.3](#) e [UC-4.8](#).

B.3.1 Mensagem DAF solicitarAutenticacao

B.3.1.1 Pedido - mensagem 2

Listagem B.26: Documento JSON para o pedido da mensagem solicitarAutenticacao

```
1 {  
2   "msg": 3  
3 }
```

B.3.1.2 Resposta - mensagem 3

Listagem B.27: Documento JSON para a resposta da mensagem solicitarAutenticacao

```
1 {  
2   "res":0,  
3   "nnc":"iWL3iQb36uMk0BFyzlU5PQ"  
4 }
```

B.3.2 Mensagem DAF autorizarDFE

B.3.2.1 Pedido - mensagem 4

Na Listagem B.28 e na Listagem B.29 é apresentado o DF-e e o conjunto de informações essenciais, respectivamente, utilizados no pedido da mensagem autorizarDFE apresentado na Listagem B.30.

Listagem B.28: Documento XML de uma NFC-e para o pedido da mensagem autorizarDFE

```
1 <infNFe Id="NFe42210328572444000110650015259564581225112940" versao="4.00"><ide><cUF>42</cUF><CNF>  
2 22511294</CNF><natOp>VENDA DE MERCADORIA CONFORME CFOP</natOp><mod>65</mod><serie>0</serie><  
3 nNF>525956458</nNF><dhEmi>2021-3-13T12:01:02-03:00</dhEmi><tpNF>1</tpNF><idDest>1</idDest><  
4 cMunFG>4205407</cMunFG><tpImp>5</tpImp><tpEmis>1</tpEmis><cDV>0</cDV><tpAmb>1</tpAmb><finNFe>1  
5 </finNFe><indFinal>1</indFinal><indPres>1</indPres><procEmi>0</procEmi><verProc>NFC-e 1.03</  
6 verProc></ide><emit><CNPJ>28572444000110</CNPJ><xNome>NOME DO ESTABELECIMENTO COMERCIAL</  
7 xNome><enderEmit><nro>999</nro><xCpl>SALA 1</xCpl><xBairro>BAIRRO</xBairro><cMun>4205407</  
8 cMun><xMun>Floriano<poli<polis></xMun><UF>SC</UF><CEP>88010000</CEP><cPais>1058</cPais><xPais>BRASIL<  
9 /xPais><fone>9999999999</fone></enderEmit><IE>9999999999</IE><CRT>1</CRT></emit><dest><CPF>  
10 53939762083</CPF><xNome>nome do cliente</xNome><indIEDest>9</indIEDest><email>email@cliente.  
11 com</email></dest><det nItem="1"><prod><cProd>PI3199</cProd><cEAN>SEM GTIN</cEAN><xProd>NOME  
12 DO PRODUTO</xProd><NCM>70099200</NCM><CEST>1008000</CEST><CFOP>5405</CFOP><uCom>UN</uCom><  
13 qCom>1.0000</qCom><vUnCom>229.9000000000</vUnCom><vProd>229.90</vProd><cEANTri<b>SEM GTIN</  
14 cEANTri<b><uTri<b>UN</uTri<b><qTri<b>1.0000</qTri<b><vUnTri<b>229.9000</vUnTri<b><indTot>1</indTot></  
15 prod><imposto><vTotTri<b>87.64</vTotTri<b><ICMS><ICMSSN500><orig>1</orig><CSOSN>500</CSOSN></  
16 ICMSSN500></ICMS><PIS><PISNT><CST>08</CST></PISNT></PIS><COFINS><COFINSNT><CST>08</CST></  
17 COFINSNT></COFINS></imposto></det><total><ICMSTot><vBC>0.00</vBC><vICMS>0.00</vICMS><  
18 vICMSDeson>0.00</vICMSDeson><vFCP>0.00</vFCP><vBCST>0.00</vBCST><vST>0.00</vST><vFCPST>0.00</  
19 vFCPST><vFCPSTRet>0.00</vFCPSTRet><vProd>229.90</vProd><vFrete>0.00</vFrete><vSeg>0.00</vSeg><  
20 vDesc>0.00</vDesc><vII>0.00</vII><vIPI>0.00</vIPI><vIPIDevol>0.00</vIPIDevol><vPIS>0.00</vPIS>  
21 <vCOFINS>0.00</vCOFINS><vOutro>0.00</vOutro><vNF>229.90</vNF><vTotTri<b>87.64</vTotTri<b></  
22 ICMSTot></total><transp><modFrete>9</modFrete></transp><pag><detPag><tPag>03</tPag><vPag>  
23 229.90</vPag><card><tpIntegra>2</tpIntegra><CNPJ>81372046000133</CNPJ><tBand>02</tBand><cAut>  
24 MQ13X1XB</cAut></card></detPag></pag><infRespTec><CNPJ>71035546000126</CNPJ><xContato>nome do  
25 responsavel</xContato><email>email@responsavel.com</email><fone>9999999999</fone></  
26 infRespTec></infNFe>
```

Listagem B.29: Fragmento XML com conjunto de informações essenciais de uma NFC-e para o pedido da mensagem autorizarDFE

```

1 <infNFe Id="NFe42210328572444000110650015259564581225112940" versao="4.00"><ide><cUF>42</cUF><cNF>
  22511294</cNF><natOp>VENDA DE MERCADORIA CONFORME CFOP</natOp><mod>65</mod><serie>0</serie><
  nNF>525956458</nNF><dhEmi>2021-3-13T12:01:02-03:00</dhEmi><tpNF>1</tpNF><idDest>1</idDest><
  cMunFG>4205407</cMunFG><tpImp>5</tpImp><tpEmis>1</tpEmis><cDV>0</cDV><tpAmb>1</tpAmb><finNFe>1
  </finNFe><indFinal>1</indFinal><indPres>1</indPres><procEmi>0</procEmi><verProc>NFC-e 1.03</
  verProc></ide><total><ICMSTot><vBC>0.00</vBC><vICMS>0.00</vICMS><vICMSDeson>0.00</vICMSDeson><
  vFCP>0.00</vFCP><vBCST>0.00</vBCST><vST>0.00</vST><vFCPST>0.00</vFCPST><vFCPSTRet>0.00</
  vFCPSTRet><vProd>229.90</vProd><vFrete>0.00</vFrete><vSeg>0.00</vSeg><vDesc>0.00</vDesc><vII>
  0.00</vII><vIPI>0.00</vIPI><vIPIDevol>0.00</vIPIDevol><vPIS>0.00</vPIS><vCOFINS>0.00</vCOFINS>
  <vOutro>0.00</vOutro><vNF>229.90</vNF><vTotTrib>87.64</vTotTrib></ICMSTot></total></infNFe>

```

Listagem B.30: Documento JSON para o pedido da mensagem autorizarDFE

```

1 {
2   "msg": 4,
3   "fdf": "PGluZk5GZSB2ZXJzYW98IjQuMDAiIElkPSJORmUOMjIxMDMyODU3MjQONDAwMDExMDY1MDAxNTI1OTU2ND
  U4MTIyNTEwMjM0MCI-PG1kZT48Y1VGPjQyPC9jVUY-PGNORj4yMjUxMTI5NDwvY05GPjxuYXRPCD5WRU5EQSBERBn
  RVJDQRPUk1BIENPTkZPuk1FIENGT1A8L25hdE9wPjxtb2Q-NjU8L21vZD48c2VyaWU-MDwvc2VyaWU-PG50Rj41Mj
  U5NTYONTg8L250Rj48ZGhfFbWk-MjAyMS0zL2EzVDEyOjAxOjAyLTAzOjAwPC9kaEVtaT48dHBORj4xPC90cE5GPjxp
  ZERlc3Q-MTwwaWREZXRNPjxjTXVurkc-NDIwNTQwNzwwY011bkZHPjx0cEltcD41PC90cEltcD48dHBFbWlZPjE8L3
  RWRW1pcz48YORWPjA8L2NEVj48dHBBbWI-MTwwdHBBbWI-PGZpbk5GZT4xPC9maW50RmU-PG1uZEZpbmFsPjE8L21u
  ZEZpbmFsPjxpbmRQcmVzPjE8L21uZFBYzXM-PHByb2NFBWk-MDwvcHJvY0VtaT48dmVvUHJvYz50RkMtZSAxLjAzP
  C92ZXJQcm9jPjwvRWR1Pjx0b3RhbD48SUNNU1RvdD48dkJDPjAuMDA8L3ZCQz48dk1DTVM-MC4wMDwvdk1DTVM-PHZ
  JQ01TRGVzb24-MC4wMDwvdk1DTVNEZXRnbj48dkZDUD4wLjAwPC92RkNQPjx2QkNTVD4wLjAwPC92QkNTVD48d1NUP
  jAuMDA8L3ZTVD48dkZDUFNUPjAuMDA8L3ZGQ1BTVD48dkZDUFNUUvOPjAuMDA8L3ZGQ1BTVFJldD48d1Byb2Q-MjI5
  LjkwPC92UHJvZD48dkZyZXR1PjAuMDA8L3ZGcmVOZT48d1N1Zz4wLjAwPC92U2VnPx2RGVzYz4wLjAwPC92RGVzY
  z48dk1JPjAuMDA8L3ZJST48dk1QST4wLjAwPC92SVBjPjx2SVBjRGV2b2w-MC4wMDwvdk1QSURldm9sPjx2UE1TPjA
  uMDA8L3ZQSVM-PHZDZ0ZJTL1M-MC4wMDwvdk1NPRk1OUz48dk91dHJvPjAuMDA8L3ZPdXRybz48dk5GPjIyOS45MDwvd
  k5GPjx2VG90VHJpYj44Ny42NDwvd1RvdFRyYWI-PC9JQ01TVG90PjwvdG90YWw-PC9pbmZORmU-",
4   "hdf": "kNmqhXlas2WuN3fb9DupbgGkTrqU4N6a6T6DzzGAiK8",
5   "pdv": "x4YowJo6Xs",
6   "red": "Gx-eNqDRJm3IGFmXq-dughS0wPGIPhnc9ZAIzhWl1Fk"
7 }

```

B.3.2.2 Resposta - mensagem 6

O DAF irá gerar um *token* JWT que deverá ser incorporado na resposta da mensagem. A Listagem B.31 apresenta o cabeçalho e o conteúdo (veja Tabela 6.8) para a geração do *token* JWT. Neste exemplo, o *token* JWT é assinado com a chave SEF. A resposta da mensagem é apresentada na Listagem B.32.

Listagem B.31: Cabeçalho e conteúdo do *token* JWT que será incorporado na resposta da mensagem autorizarDFE

```

1 {
2   "typ": "JWT",
3   "alg": "HS256"
4 }
5 {
6   "daf": "YRaQYtWtROCSI-gCuL7oyg",

```



```

7     <chDFe>42210328572444000110650015259564581225112940</chDFe>
8     <idAut>URl1rnf8wxxstXJ7PofbotVlMi4GpJP60dBd0pGh04yE</idAut>
9     <hAut>VTK41YsrqJ3eBAQoSXlZM_-rZSBquMBTXDdzF74wsuU</hAut>
10    <cStatAut>1005</cStatAut>
11    <xMotAut>Validação do fragmento DAF realizada com sucesso</xMotAut>
12  </retDFe>
13 </retAutorizacao>
14 </obterResultadoAutorizacaoResponse>

```

B.4.2 Mensagem DAF apagarAutorizacaoRetida

B.4.2.1 Pedido - mensagem 4

Listagem B.35: Documento JSON para o pedido da mensagem apagarAutorizacaoRetida

```

1 {
2   "msg": 5,
3   "aut": "URl1rnf8wxxstXJ7PofbotVlMi4GpJP60dBd0pGh04yE",
4   "apg": "VTK41YsrqJ3eBAQoSXlZM_-rZSBquMBTXDdzF74wsuU"
5 }

```

B.4.2.2 Resposta - mensagem 6

Listagem B.36: Documento JSON para a resposta da mensagem apagarAutorizacaoRetida

```

1 {
2   "res": 0
3 }

```

B.5 Solicitar remoção extraordinária de autorizações retidas no DAF

Os exemplos apresentados referem-se ao processo para solicitação extraordinária de exclusão de autorizações retidas na MT do DAF como descrito na [Subseção 7.6.11](#).

B.5.1 Mensagem DAF consultarInformacoes

B.5.1.1 Pedido

Listagem B.37: Documento JSON para o pedido da mensagem consultarInformacoes

```

1 {
2   "msg": 8
3 }

```



```
5 <xMotivo>Solicitação recebida com sucesso</xMotivo>
6 <nRec>202105101009210</nRec>
7 <retDFe>
8 <chDFe>42210528572444000110650010125656651776083824</chDFe>
9 <idAut>URlrnf8wxxstXJ7PofbotV1Mi4GpJP60dBdOpGh04yE</idAut>
10 <hAut>VTK41YsrqJ3eBAQoSX1ZM_-rZSBquMBTXDdzF74wsuU</hAut>
11 <cStatAut>1005</cStatAut>
12 <xMotAut>Validação do fragmento DAF realizada com sucesso</xMotAut>
13 </retDFe>
14 </retConsAutApagar>
15 </consultarAutorizacaoApagarResponse>
```

B.5.5 Mensagem DAF apagarAutorizacaoRetida

B.5.5.1 Pedido

Listagem B.45: Documento JSON para o pedido da mensagem apagarAutorizacaoRetida

```
1 {
2   "msg": 5,
3   "aut": "URlrnf8wxxstXJ7PofbotV1Mi4GpJP60dBdOpGh04yE",
4   "apg": "VTK41YsrqJ3eBAQoSX1ZM_-rZSBquMBTXDdzF74wsuU"
5 }
```

B.5.5.2 Resposta

Listagem B.46: Documento JSON para a resposta da mensagem apagarAutorizacaoRetida

```
1 {
2   "res": 0
3 }
```

C Pseudocódigos para representação das máquinas de estado do PDAF-CDC

Os pseudocódigos disponibilizados neste apêndice buscam apoiar e fornecer um guia para a compreensão e implementação dos diagramas de máquinas de estados finitos apresentados na [Subseção 6.2.2](#) e [Subseção 6.2.3](#).

No [algoritmo 1](#) e [algoritmo 2](#) são apresentados pseudocódigos dos estados Ocioso e Espera, respectivamente, da máquina de estados finitos da camada de Garantia de entrega do PDAF-USB, apresentada na [Figura 6.3](#).

No [algoritmo 3](#), [algoritmo 4](#) e [algoritmo 5](#) são apresentados pseudocódigos dos estados Ocioso, Tamanho e RX, respectivamente, da máquina de estados finitos da camada de Enquadramento do PDAF-USB, apresentada na [Figura 6.4](#).

Algoritmo 1: Estado *Ocioso* da máquina de estados finitos da Garantia de entrega

```
1 seqRX = 0;
2 seqTX = 0;
3 enquanto está no estado Ocioso faça
4     se recebe Dados da camada superior API-DAF;
5     então
6         monta um quadro anexando o campo Controle do tipo DATA, com o respectivo número
           de sequência de transmissão (veja Tabela 6.22), aos dados recebidos;
7         tentativas = 0;
8         armazena o quadro enviado e o mantém como pendente;
9         envia o quadro para a camada inferior Enquadramento;
10        habilita o timeout;
11        muda para o estado Espera;
12    senão
13        se recebe um quadro da camada inferior Enquadramento com o campo Controle do
           tipo DATA;
14        então
15            se DATA possui número de sequência esperado;
16            então
17                monta um quadro contendo apenas ACK_seqRX, onde seqRX corresponde ao
                   número de sequência recebido (veja Tabela 6.22);
18                seqRX = 1 - seqRX;
19                envia o quadro com ACK para a camada inferior Enquadramento;
20                extrai e envia o campo Dados do quadro recebido para a camada superior
                   API-DAF;
21            senão
22                monta um quadro contendo apenas ACK_seqRX, onde seqRX corresponde ao
                   número de sequência recebido (veja Tabela 6.22);
23                envia o quadro com ACK para a camada inferior Enquadramento;
24            fim
25        fim
26    fim
27 fim
```

Algoritmo 2: Estado Espera da máquina de estados finitos da Garantia de entrega

```
1 enquanto está no estado Espera faça
2   se recebe um quadro da camada inferior Enquadramento com o campo Controle do tipo
   ACK com o número de sequência de transmissão esperado;
3   então
4     seqTX = 1 - seqTX;
5     desabilita o timeout;
6     muda para o estado Ocioso;
7   senão se recebe um quadro da camada inferior Enquadramento com o campo Controle do
   tipo ACK com o número de sequência de transmissão não esperado ou foi gerado um
   timeout;
8   então
9     se tentativas == ao máximo de tentativas;
10    então
11      desabilita o timeout;
12      muda para o estado Ocioso;
13    senão
14      tentativas = tentativas + 1;
15      reinicia o timeout;
16      reenvia mensagem pendente para a camada inferior Enquadramento;
17    fim
18  senão
19    se recebe um quadro da camada inferior Enquadramento com o campo Controle do
   tipo DATA;
20    então
21      se DATA possui número de sequência esperado;
22      então
23        monta um quadro contendo apenas ACK_seqRX, onde seqRX corresponde ao
        número de sequência recebido (veja Tabela 6.22);
24        seqRX = 1 - seqRX;
25        envia o quadro com ACK para a camada inferior Enquadramento;
26        extrai e envia o campo Dados do quadro recebido para a camada superior
        API-DAF;
27      senão
28        monta um quadro contendo apenas ACK_seqRX, onde seqRX corresponde ao
        número de sequência recebido (veja Tabela 6.22);
29        envia o quadro com ACK para a camada inferior Enquadramento;
30      fim
31    fim
32  fim
33 fim
```

Algoritmo 3: Estado Ocioso da máquina de estados finitos da camada de Enquadramento

```
1 qtde_bytes_campo_tamanho = 0;
2 enquanto está no estado Ocioso;
3 faça
4     recebe um byte;
5     se byte recebido está presente na Tabela 6.20;
6     então
7         se byte recebido == ao byte do comando enviarMensagem;
8         então
9             qtde_bytes_campo_tamanho = 2;
10        senão
11            qtde_bytes_campo_tamanho = 4;
12        fim
13        habilita o timeout;
14        muda para o estado Tamanho;
15    fim
16 fim
```

Algoritmo 4: Estado Tamanho da máquina de estados finitos da camada de Enquadramento

```
1 tamanho_inteiro = 0;
2 bytearray buffer_tamanho = 0;
3 enquanto está no estado Tamanho faça
4     se timeout é gerado;
5     então
6         desabilita o timeout;
7         muda para o estado Ocioso;
8     senão
9         recebe um byte;
10        /* variável qtde_bytes_campo_tamanho definida no algoritmo 3 */
11        se total de bytes recebidos no buffer_tamanho == qtde_bytes_campo_tamanho - 1;
12        então
13            anexa o byte recebido no buffer_tamanho;
14            reinicia o timeout;
15            tamanho_inteiro = (int) buffer_tamanho;
16            muda para o estado RX ;
17        senão
18            anexa o byte recebido no buffer_tamanho;
19            reinicia o timeout;
20        fim
21    fim
22 fim
```

Algoritmo 5: Estado RX da máquina de estados finitos da camada de Enquadramento

```
1 bytearray buffer_dados = 0;
2 enquanto está no estado RX faça
3     se timeout é gerado;
4     então
5         desabilita o timeout;
6         muda para o estado Ocioso ;
7     senão
8         recebe um byte;
9         /* variável tamanho_inteiro definida no algoritmo 4 */
10        se a quantidade de bytes no buffer_dados == tamanho_inteiro - 1;
11        então
12            anexa o byte recebido no buffer_dados;
13            desabilita o timeout;
14            envia o buffer_dados e o byte Comando para a camada superior Garantia de
15            entrega;
16            muda para o estado Ocioso;
17        senão
18            anexa o byte recebido no buffer_dados;
19            reinicia o timeout;
20        fim
21    fim
```
