DISPOSITIVO AUTORIZADOR FISCAL

Especificação Técnica de Requisitos

Revisão: CP 001

23 de novembro de 2020

Histórico de revisões

Revisão	Data	Descrição
CP 001	23.11.2020	Versão inicial para consulta pública

Sumário

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.

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).

JSON *JavaScript Object Notation*.

JWK *JSON Web Key*.

JWT *JSON Web Token*.

LED Diodo Emissor de Luz.

MEU *Memory Encryption Unit* (*Veja: Memory Encryption Unit*).

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

NFC-e Nota Fiscal de Consumidor Eletrônica.

PAF Programa Aplicativo Fiscal.

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

PEM *Privacy Enhanced Mail)*.

PKCS *Public Key Cryptography Standards*.

RFC *Request for Comments*.

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*).

UF Unidade Federada.

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

Aceleração criptográfica em *hardware* módulo de *hardware* interno ao microcontrolador seguro específico para auxiliar a execução ou executar completamente as rotinas criptográficas.

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 e enviada por um emissor, 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. Tem a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves (pública/privada).

Bootloader reúne o sistema básico executado imediatamente após a inicialização do processador.

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 critográfica 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 pela chave pública correspondente.

Chave privada do DAF chave privada gerada pela rotina de registro do Dispositivo Autorizador Fiscal (DAF) junto à SEF.

Chave pública chave critográfica 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.

Escudo ativo antiviolação sensor de malha antiviolação que cobre uma região interna ao encapsulamento de um circuito integrado, fornecendo resistência e detecção à violação, bem como evidência de que uma violação ocorreu. Pode também fornecer resposta à violação, como por exemplo zerar uma região de memória imediatamente após a detecção.

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).

Memory Encryption Unit unidade de criptografia de memória, baseada em algoritmo de chave simétrica, responsável por cifrar de maneira transparente ao usuário, os dados escritos e lidos em uma determinada região de memória não volátil.

Modo inutilizado conjunto de rotinas que implementa 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

Lista de Tabelas

Lista de Códigos

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.

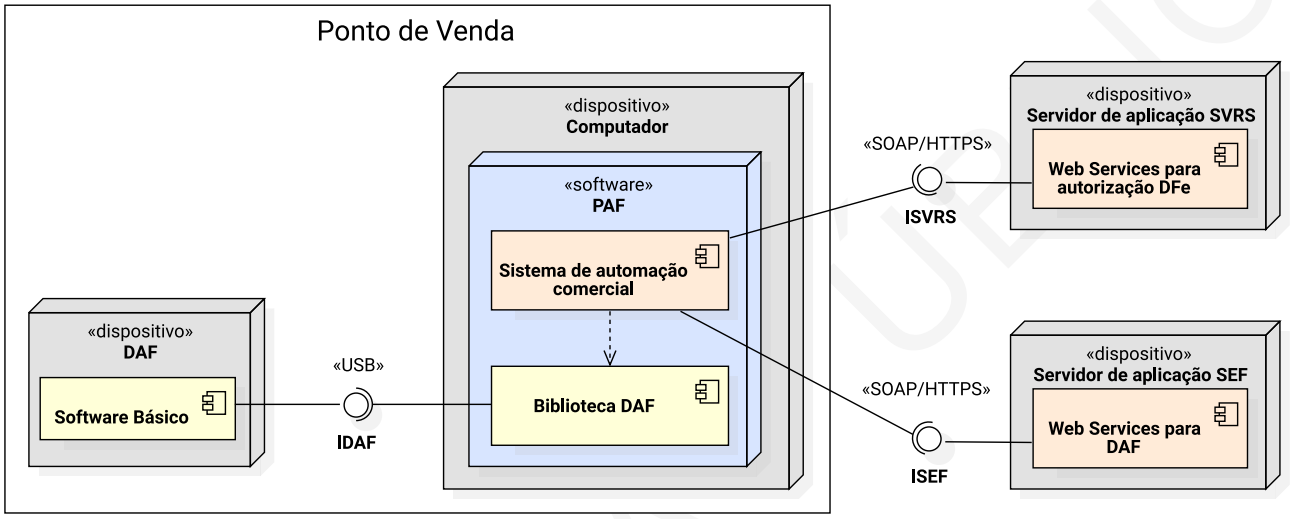
De acordo com a decisão do Grupo Especialista Setorial em Automação Comercial da SEF (GESAC), o DAF deverá ser capaz de autorizar os seguintes documentos Bilhete de Passagem Eletrônico (BP-e) (ENCAT, 2019b) e Nota Fiscal de Consumidor Eletrônica (NFC-e) (ENCAT, 2019a), uma vez que a emissão desses pode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

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. De acordo com os requisitos apresentados pelo GESAC, cada Ponto de Venda

(PDV) terá um DAF próprio, sendo esse comandado por seu PAF. Dessa forma, entende-se que um contribuinte terá um par PAF e DAF para cada PDV em seu estabelecimento.

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, 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



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.

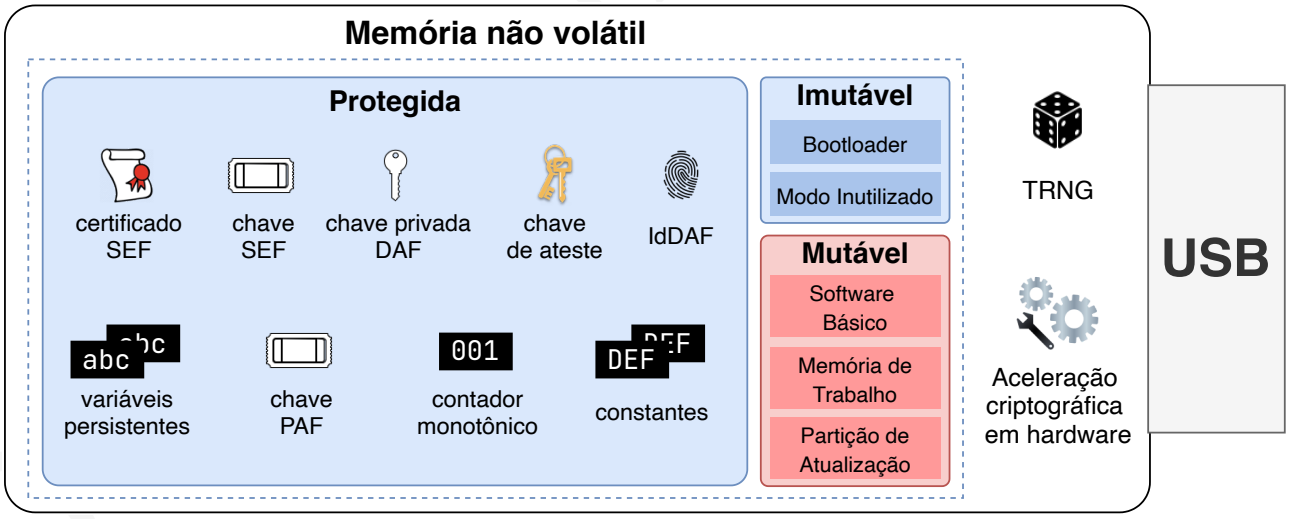
2 Visão geral do DAF

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 será apresentada uma visão de alto nível do DAF. De uma forma geral, serão 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 dos componentes do DAF com os principais componentes e artefatos.

Figura 2.1: Visão geral dos componentes do DAF.



Abaixo são descritos os principais componentes do DAF:

- *Bootloader* - reúne o sistema básico executado imediatamente após a inicialização do processador;
- Modo inutilizado - conjunto de rotinas que implementa 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;
- Aceleração criptográfica em *hardware* - módulo de *hardware* interno ao microcontrolador seguro específico para auxiliar a execução ou executar completamente as rotinas criptográficas.

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.

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 5.5). Além disso, também será utilizado no processo de atualização do próprio certificado (Veja Seção 5.6).

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, poderá recorrer à rotina específica da SEF para recuperar a cópia da mesma (Veja Subseção 7.6.5 e Seção 8.13).

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 5.4), 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 no caso do limite de autorizações retidas for atingido, ou seja, `numDFe >= Max` (Veja Seção 5.2 e Caso de Uso UC-4.2);
- 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-4.1).

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. Essa 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

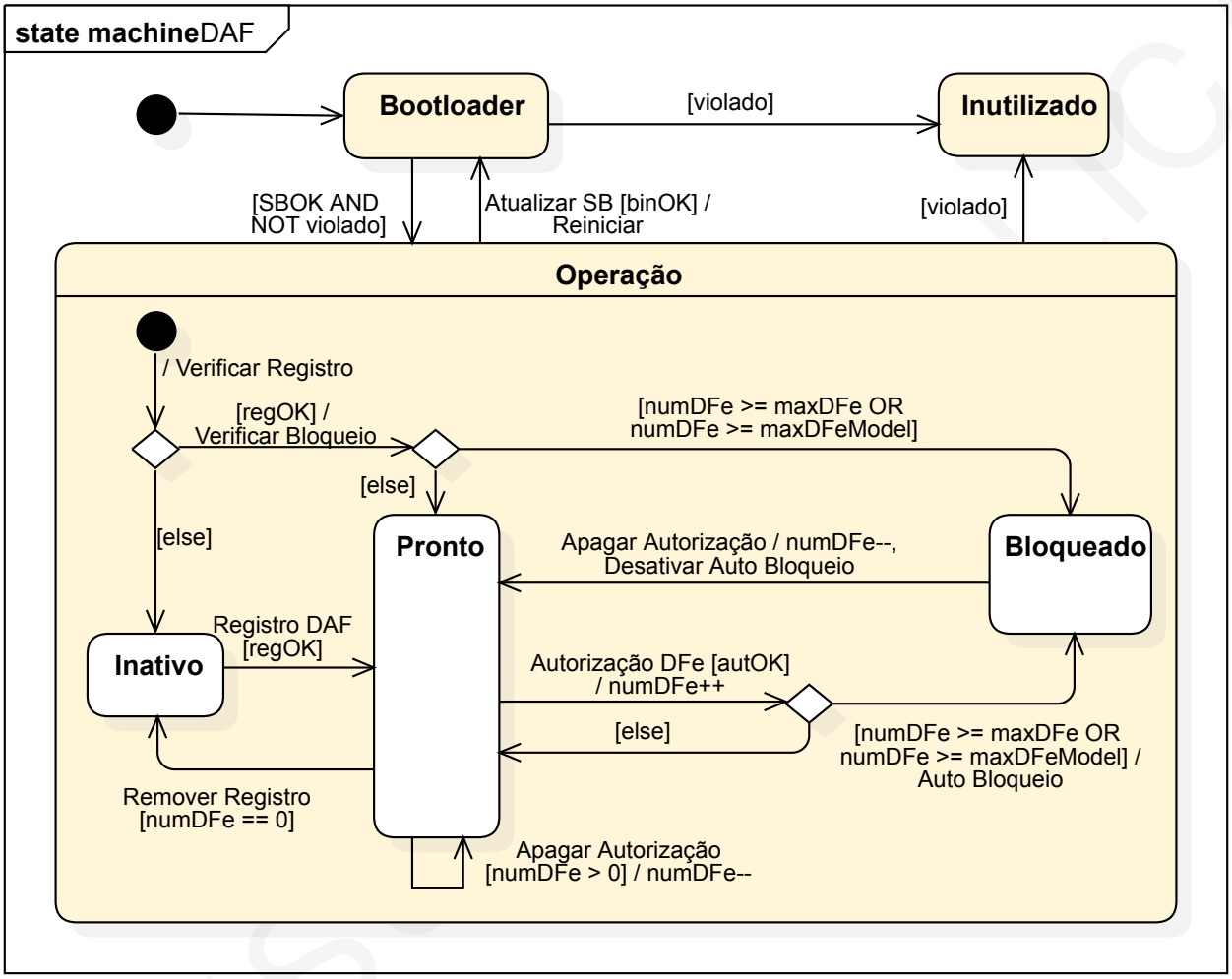


Tabela 2.1: Condições de guarda

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.

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

`maxDFe`	∞	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. Uma vez verdadeiro, esse indicador 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	Comentário
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 5.4), no qual não pode haver autorizações retidas na memória do DAF (`numDFe == 0`).
Autorização DFe	PRONTO → BLOQUEADO	Processo de autorização de um DF-e (Veja Seção 5.2) quando pelo menos um dos limites máximos (`maxDFe` ou `maxDFeModel`) é alcançado e o auto-bloqueio é ativado (Veja Caso de Uso UC-4.2).
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-4.7).
Atualizar SB	OPERAÇÃO → BOOTLOADER	Processo de atualização do SB (Veja Seção 5.5), quando o *Software* Básico Candidato é valido 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 encontrata na Seção 4.3.

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-4.5). Enquanto as outras duas partições armazenam o SB e, quando for o caso, a imagem de atualização assinada pela SEF, 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 escudo ativo antiviolação, memória criptografada e sensores ambientais. 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 Permanente
Condições de guarda	`maxDFeModel`	✓	
(Veja Tabela 2.1)	`maxDFe`		✓
	`regOK`		✓
	`numDFe`		✓
	`violado`		✓
Artefatos	Certificado digital da SEF		✓
(Veja Seção 2.1)	Chave privada do DAF		✓
	Chave SEF		✓
	Chave PAF		✓
	Contador monotônico		✓
	Chave de ateste	✓	
	IdDAF	✓	
Parâmetros de atualização	Resumo criptográfico do SB		✓
(Veja Seção 5.5)	Versão do SB		✓

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

Nessa 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 ser uma chave RSA de 4.096 bits.
2. Chave privada do DAF DEVE ser uma chave RSA de 2.048 bits.
3. Chave SEF é um valor arbitrário de 512 bits e DEVE ser mantida somente no DAF e na SEF.
4. Chave PAF é um valor arbitrário de 512 bits e DEVE ser mantida no DAF, no PAF e na SEF.
5. Os resumos criptográficos DEVEM ser gerados com a função SHA-256 (NIST, 2015).
6. As assinaturas digitais usando a chave privada do DAF DEVEM ser geradas dentro do ambiente de execução do microcontrolador seguro.
    6.1. A suíte de assinatura DEVE ser `sha256WithRSAEncryption` (MORIARTY et al., 2016).
7. O certificado digital da SEF seguirá as especificações da ICP-Brasil (ICP-BRASIL, 2019, 2020), porém PODE ser auto-asssinado (quando incluído em tempo de manufatura do DAF) ou PODE ter sido emitido por uma Autoridade Certificadora (AC) mantida ou indicada pela SEF.
8. 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.
9. 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.
    9.1. Na interação entre DAF e SEF, a chave SEF DEVE ser usada como a chave secreta do HMAC;
    9.2. Na interação entre PAF e DAF, a chave secreta do HMAC DEVE ser a chave PAF.
10. 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.

11. O IdDAF DEVE ser um *Universally Unique Identifier* (UUID) (LEACH; MEALLING; SALZ, 2005) da versão 1, 4 ou 5.
    11.1. 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

```
import uuid
# Criar o namespace da versão 5 com o nome de domínio do fabricante
dominio = uuid.uuid5(uuid.NAMESPACE_DNS,'fabricante.exemplo.com.br')

# Criar uuid a partir do domínio e name. No caso, name é uma string única por DAF
daf_modeloa_serie_1234 = uuid.uuid5(dominio,'modeloA+1234')
```

12. 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

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

2.4.4 Requisitos da memória mutável

18. A região de memória mutável DEVE prever as partições MT, de armazenamento do SB e a partição de atualização.
19. DEVE ser não volátil.
20. PODE ser implementada por um ou mais componentes físicos de memória.
21. A partição MT:
    21.1. DEVE ser utilizada para armazenar as informações fiscais referente ao caso de uso Autorizar DF-e (UC-4.5) até a sua devida remoção (Veja UC-4.1);
    21.2. DEVE possuir capacidade mínima de armazenar `maxDFe` autorizações (Veja Tabela 2.1);
    21.3. DEVE possuir vida útil para armazenar no mínimo 10.000 $\times$ `maxDFe` de autorizações;
    21.4. PODE ser implementada por um *chip* externo ao processador.
22. A partição do *Software* Básico:
    22.1. DEVE permitir escrita somente pelo *bootloader*;
    22.2. DEVE conter exclusivamente as instruções do SB.
23. A partição de atualização PODE ser implementada por um *chip* externo ao processador.
24. A MT e a partição de atualização PODEM ser implementadas no mesmo chip.

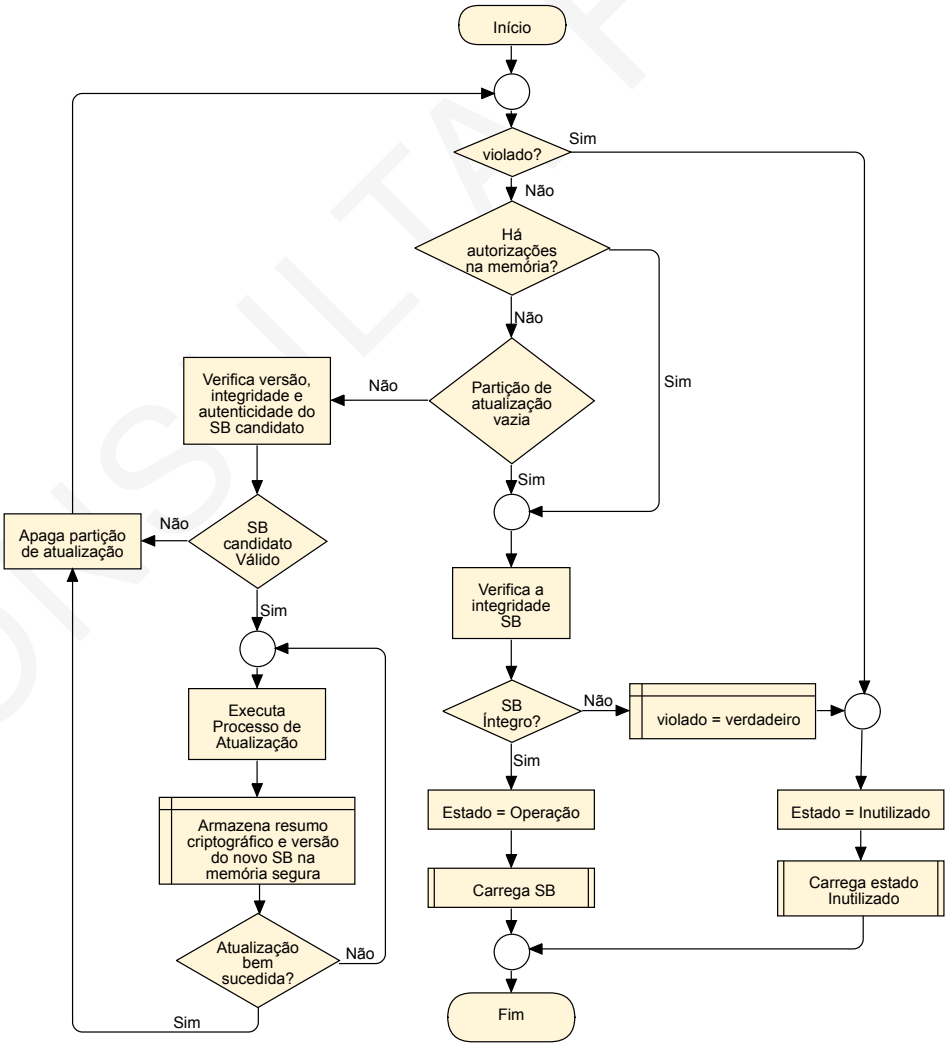
2.4.5 Requisitos da memória protegida

25. A região de memória protegida DEVE ser não volátil.
26. DEVE possuir escudo ativo antiviolação.
27. DEVE armazenar as informações apresentadas na Tabela 2.3.
28. DEVE ser cifrada por uma *Memory Encryption Unit* (MEU) com os seguintes requisitos:
    - 28.1. A MEU DEVE ser baseada em algoritmo de criptografia de chave simétrica reconhecidamente seguro pelo mercado;
    - 28.2. A chave simétrica utilizada para cifragem DEVE ser exclusiva à MEU e sem acesso via *software*.

2.4.6 Requisitos do *bootloader*

As operações executas 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:

29. DEVE ser o único ponto de entrada após o reinício do DAF.
30. DEVE ser armazenado na região imutável (Veja Subseção 2.4.3).
31. DEVE implementar o comportamento especificado na Figura 2.3.

2.4.7 Requisitos do modo inutilizado

32. O modo inutilizado DEVE ser armazenado na memória imutável (Veja Subseção 2.4.3).
33. DEVE ser executado imediatamente após a detecção de uma violação.
34. DEVE ser irreversível e persistente.
35. DEVE implementar comunicação unidirecional do DAF para o *host*, pela interface de comunicação definida na Seção 3.7.
36. NÃO DEVE implementar nenhum protocolo interativo, incluindo o protocolo descrito no Capítulo 6.
37. DEVE enviar uma única vez, 30 segundos após entrar no estado INUTILIZADO, as informações abaixo:
    - 37.1. Conteúdo da partição do SB;
    - 37.2. Conteúdo da MT;
    - 37.3. Os seguinte valores armazenados na memória protegida:
        - 37.3.1. `maxDFeModel`;
        - 37.3.2. `maxDFe`;
        - 37.3.3. `regOK`;
        - 37.3.4. `numDFe`;
        - 37.3.5. contador monotônico;
        - 37.3.6. IdDAF;
        - 37.3.7. Resumo criptográfico do SB;
        - 37.3.8. Versão do SB.
    - 37.4. As informações DEVEM ser transmitidas na ordem que aparecem no item anterior e DEVEM ser representadas como uma cadeia de caracteres hexadecimais, separadas pelo caractere de barra vertical (*pipe*).

2.4.8 Requisitos do *software* básico

38. O SB DEVE ser executado somente após o resultado positivo da verificação da integridade executada pelo *bootloader*.
39. DEVE ser armazenado na região mutável (Veja Subseção 2.4.4).

40. DEVE implementar o comportamento da máquina de estado para os estados OPERAÇÃO e seus subestados (Veja Seção 2.2).

41. DEVE ser implementado seguindo o Capítulo 4, Capítulo 5 e Capítulo 6.

2.4.9 Requisitos para atualização do SB

42. O *Software* Básico Candidato DEVE conter a versão, o resumo criptográfico e assinatura digital gerada pela SEF sobre o SBC embutidos na imagem.

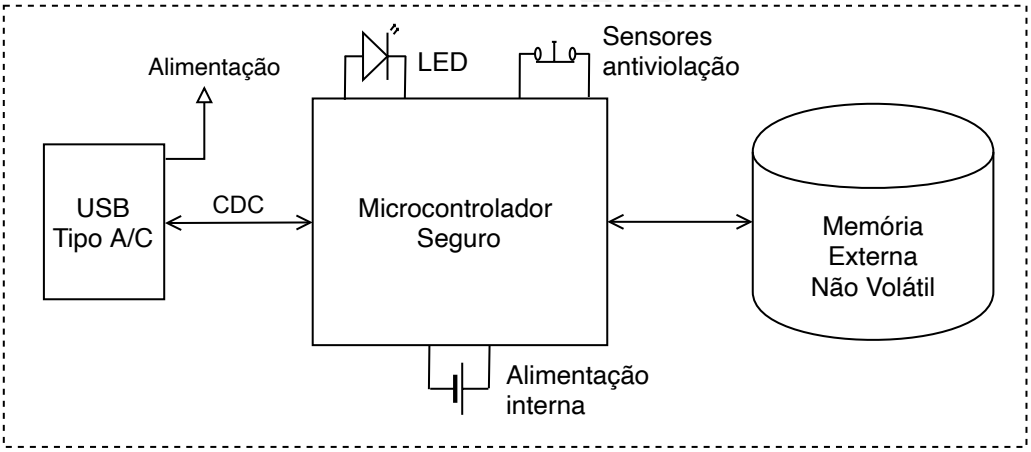
43. DEVE conter o `maxDFe` se exigido pela SEF.

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 apresentandos os componentes de *hardware* com detalhamento das interligações e os requisitos mínimos para manutenção das prerrogativas de segurança.

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

Figura 3.1: Organização do DAF com os componentes mínimos e suas 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

44. 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).
45. DEVE ser afixado na placa sem soquete ou conector.
46. DEVE possuir escudo ativo antiviolação.
47. DEVE possuir aceleração em *hardware* para cumprir os requisitos criptográficos estabelecidos na Subseção 2.4.1.
48. DEVE possuir um TRNG.

49. DEVE possuir os mecanismos necessários para implementar o sistema antiviolação (Veja Seção 3.5).

3.2 Memória externa não volátil

50. A organização PODE contar com um *chip* externo ao microcontrolador seguro de memória não volátil. Nesse caso, ele DEVE seguir os seguintes requisitos:
    50.1. DEVE ser afixado à placa sem uso de soquete ou conector;
    50.2. DEVE ser crifrada utilizando a chave SEF;
    50.3. 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.

51. As seguintes regiões e partições de memória DEVEM estar contidas no mesmo circuito integrado do microcontrolador seguro:
    51.1. Memória imutável (Veja Subseção 2.4.3);
    51.2. Memória protegida (Veja Subseção 2.4.5);
    51.3. Partição do SB (Veja Item 22.).
52. As seguintes partições PODEM ser implementadas na memória externa (Veja Seção 3.2) seguindo os requisitos da Seção 3.2 ou DEVEM estar contidas no circuito integrado do microcontrolador seguro.
    52.1. A partição MT (Veja Item 21.);
    52.2. A partição de atualização (Veja Subseção 2.4.4).

3.4 Alimentação

53. O DAF DEVE ser energizado exclusivamente pelo conector USB para a sua operação normal.
54. O DAF DEVE possuir fonte interna de energia, capaz de alimentar o sistema antiviolação enquanto não estiver ligado a uma porta USB, com as seguintes características:
    54.1. 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;
    54.2. A fonte interna de energia NÃO DEVE ser passível de substituição. (Veja Item 55. da Seção 3.5);

3.5 Gabinete e sistema antiviolação

55. O gabinete DEVE ser blindado, opaco, sem parafusos aparentes, encaixes e sem a possibilidade de abertura para qualquer tipo de manutenção.
56. O sistema antiviolação DEVE possuir as seguintes características:
    56.1. Ser composto por uma malha ativa de proteção dinâmica que cubra todos os componentes internos;
    56.2. Possuir sensores de temperatura, tensão e clock;
    56.3. Estar ativo com alimentação principal (USB) ou secundária (Veja Seção 3.4);
    56.4. Reagir imediatamente ao ser detectada qualquer violação.
57. O sistema antiviolação DEVE disparar nos seguintes casos:
    57.1. Abertura do gabinete;
    57.2. Objetos com diâmetro igual ou maior que 0,4 mm furem a malha de proteção dos componentes internos;
    57.3. Pelo menos uma das seguintes condições ocorra:
        57.3.1. Temperatura estiver fora do valor normal de operação da região de memória protegida;
        57.3.2. Alteração no escudo ativo antiviolação da memória protegida;
        57.3.3. Tensão da fonte de energia interna estiver fora do valor normal de operação.
58. Ao ser identificada uma violação, o DAF DEVE imediatamente:
    58.1. Apagar chave privada do DAF, chave de ateste e chave SEF;
    58.2. Acionar o estado INUTILIZADO (veja Seção 2.2) permitindo as funcionalidades previstas para esse estado (veja Subseção 2.4.7).
59. Os únicos componentes do DAF considerados externos são:
    59.1. Conector (plugue) USB (Veja Seção 3.7);
    59.2. LED de sinalização (Veja Seção 3.6).
60. Qualquer outro componente do DAF não listado acima é considerado um componente interno.

3.6 Sinalização

61. 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.

3.7 Interface de comunicação

62. 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.

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

63. DEVE implementar no mínimo a especificação USB 1.1 *Full Speed*;
64. DEVE ser somente do tipo dispositivo (*device*);
65. DEVE implementar a classe e subclasse USB especificadas na Seção 6.3;
66. O DAF DEVE operar sem a necessidade de instalação de *drivers* proprietários para o funcionamento junto ao PAF.

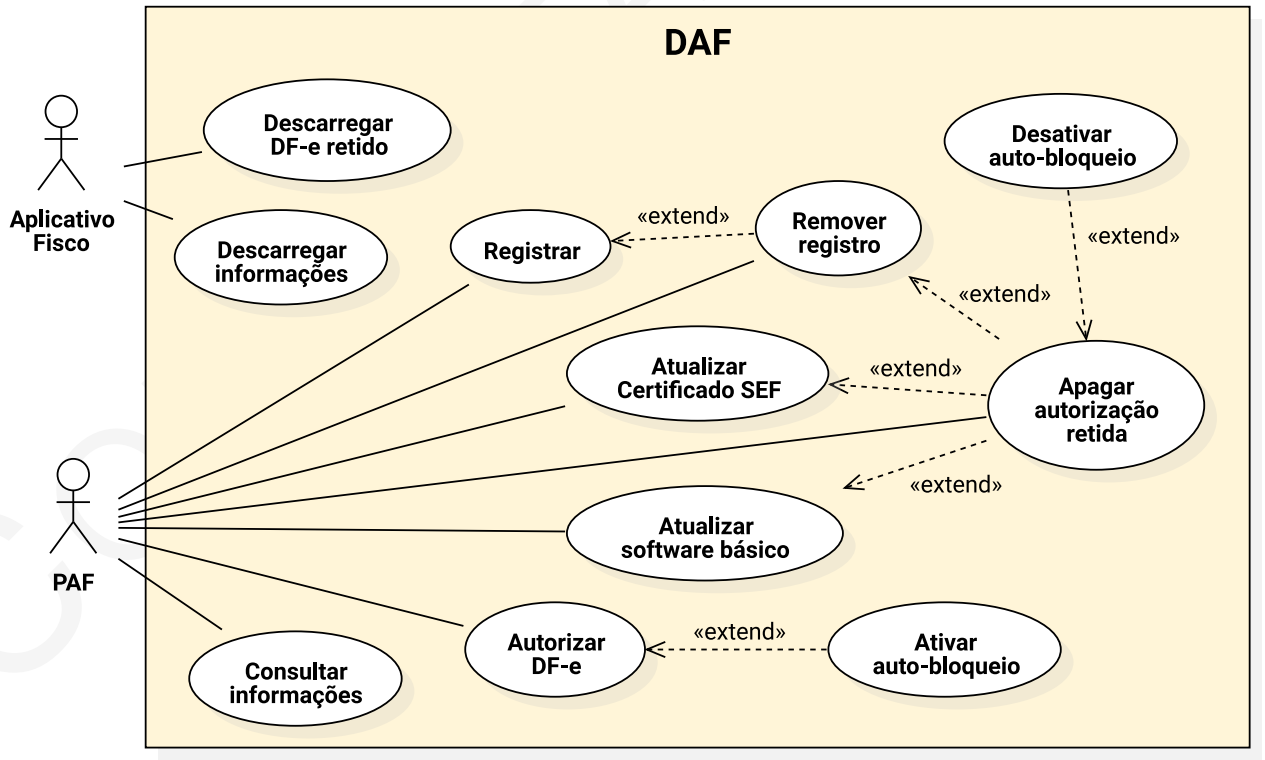
4 Software Básico

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 Fisco. Basicamente, 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 Aplicativo Fisco, utilizado 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. **Apagar autorização retida** (UC-4.1) - Para remover da MT uma autorização gerada pelo DAF e que fora processada pela SEF;
2. **Ativar auto-bloqueio** (UC-4.2) - Estende o comportamento do caso *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;

3. **Atualizar certificado SEF** (UC-4.3) - Para atualizar certificado digital da SEF armazenado no DAF;
4. **Atualizar software básico** (UC-4.4) - Para atualizar o SB do DAF;
5. **Autorizar DF-e** (UC-4.5) - Para solicitar autorização sobre um Documento Fiscal Eletrônico (DF-e) que será encaminhado à SEFAZ;
6. **Consultar informações** (UC-4.6) - Para obter informações como versão do SB, resumo criptográfico do SB, Identificador único do DAF (IdDAF), modelo, fabricante, valor atual do contador monotônico, identificadores dos documentos retidos na MT, certificado digital da SEF armazenado, estado atual do DAF e informações sobre os algoritmos criptográficos que DAF é capaz de operar;
7. **Desativar auto-bloqueio** (UC-4.7) - Estende o comportamento do caso *Apagar autorização retida* para desbloquear o DAF que fora bloqueado automaticamente pelo caso *Ativar auto-bloqueio*;
8. **Descarregar DF-e retidos** (UC-4.8) - Para permitir que o fiscal da SEF possa visualizar os conjuntos de informações essenciais dos documentos fiscais com autorizações retidas no DAF;
9. **Descarregar informações** (UC-4.9) - A ser usado pelo fiscal da SEF para obter informações como versão do SB, resumo criptográfico do SB, IdDAF, modelo, fabricante, valor atual do contador monotônico, identificadores dos documentos retidos na MT, certificado digital da SEF armazenado, estado atual do DAF e informações sobre os algoritmos criptográficos que DAF é capaz de operar. Este caso de uso segue as mesmas etapas e comandos que o Caso de Uso UC-4.6;
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: 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 Subseção 6.2.5)	
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-4.7)
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: Operação não autorizada pela SEF

1. O DAF retorna para o PAF uma mensagem de erro informando que o documento não contém permissão da SEF para a operação (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-4.2: 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-4.3: 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 Subseção 6.2.10)
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-4.1)
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 sobrescreve certificado digital da SEF
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-4.4: 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 Subseção 6.2.9)
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-4.1)
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 Subsubseção 6.3.1.2)
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 a integridade e autenticidade do SB recebido a partir da assinatura gerada pela SEF
9. O DAF informa ao PAF que o SB candidato é válido
10. 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)

UC-4.5: 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 Subseção 6.2.3)

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 resumo criptográfico do XML completo do DF-e, o conjunto de informações essenciais do DF-e (Veja Subseção 5.2.1) e código de autenticação do PAF (Veja descrição da mensagem na Subseção 6.2.4)
    - 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 atual valor de seu contador monotônico e o idAut, no caso a 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 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-4.2)

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)

UC-4.6: Consultar informações

Resumo Esse caso de uso descreve as etapas para o PAF obter informações como versão do SB, resumo criptográfico do SB, IdDAF, modelo, fabricante, valor atual do contador monotônico, certificado digital da SEF armazenado, estado do DAF, algoritmos criptográficos que o DAF provê suporte e identificadores dos documentos retidos na MT.

Ator primário PAF

Pré-condições DAF deve estar no estado PRONTO, INATIVO ou BLOQUEADO (Veja Seção 2.2)

Fluxo principal

1. O PAF solicita ao DAF suas informações (Veja descrição da mensagem na Subseção 6.2.8)
2. O DAF retorna para o PAF o documento estruturado com suas informações

UC-4.7: Desativar auto-bloqueio

Resumo Esse caso de uso descreve as etapas para desbloquear o DAF que fora bloqueado automaticamente pelo Caso de Uso UC-4.2.

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-4.8: Descarregar DF-e retidos

Resumo Esse caso de uso descreve as etapas para permitir que o Aplicativo Fisco, utilizado pelo fiscal da SEF, possa visualizar o conjunto de informações essenciais do DF-e de uma autorização retida no DAF.

Ator primário Aplicativo Fisco

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

Fluxo principal

1. O Aplicativo Fisco informa ao DAF o idAut (Veja descrição da mensagem na Subseção 6.2.11)
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 Aplicativo Fisco o conjunto de informações essenciais do DF-e

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: 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-4.9: Descarregar informações

Resumo Esse caso de uso descreve as etapas para permitir que o Aplicativo Fisco, utilizado pelo fiscal da SEF, possa obter informações como versão do SB, resumo criptográfico do SB, IdDAF, modelo, fabricante, valor atual do contador monotônico, estado do DAF, algoritmos criptográficos que o DAF provê suporte e identificadores dos documentos retidos na MT.

Ator primário	Aplicativo Fisco
Pré-condições	DAF deve estar no estado PRONTO, INATIVO ou BLOQUEADO (Veja Seção 2.2)

Fluxo principal

1. O PAF solicita ao DAF suas informações (Veja descrição da mensagem na Subseção 6.2.8)
2. O DAF retorna para o PAF o documento estruturado com suas informações

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 Subseção 6.2.1)
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) e a chave PAF (Veja descrição da mensagem na Subseção 6.2.2)
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)

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 Subseção 6.2.6)
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-4.1)
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 Subseção 6.2.7)
8. O DAF verifica se o pedido foi formado adequadamente
9. O DAF verifica se a mensagem foi assinada pela SEF
10. O DAF verifica se o documento encaminhado contém a cadeia de caracteres `REMOVER`
11. O DAF, em uma transação atômica, apaga de sua memória segura a chave privada do DAF, a chave SEF e a chave PAF
12. O DAF altera seu estado para INATIVO
13. O DAF retorna ao PAF uma mensagem informado 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: Operação não autorizada pela SEF

1. O DAF retorna para o PAF uma mensagem de erro informando que a operação não foi permitida pela SEF (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)

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
Apagar autorização retida		✓	✓
Ativar auto-bloqueio		✓	
Atualizar certificado SEF	✓	✓	
Atualizar Software Básico	✓	✓	
Autorizar DF-e		✓	
Consultar informações	✓	✓	✓
Desativar auto-bloqueio			✓
Descarregar DF-e retidos		✓	✓
Descarregar informações	✓	✓	✓
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:

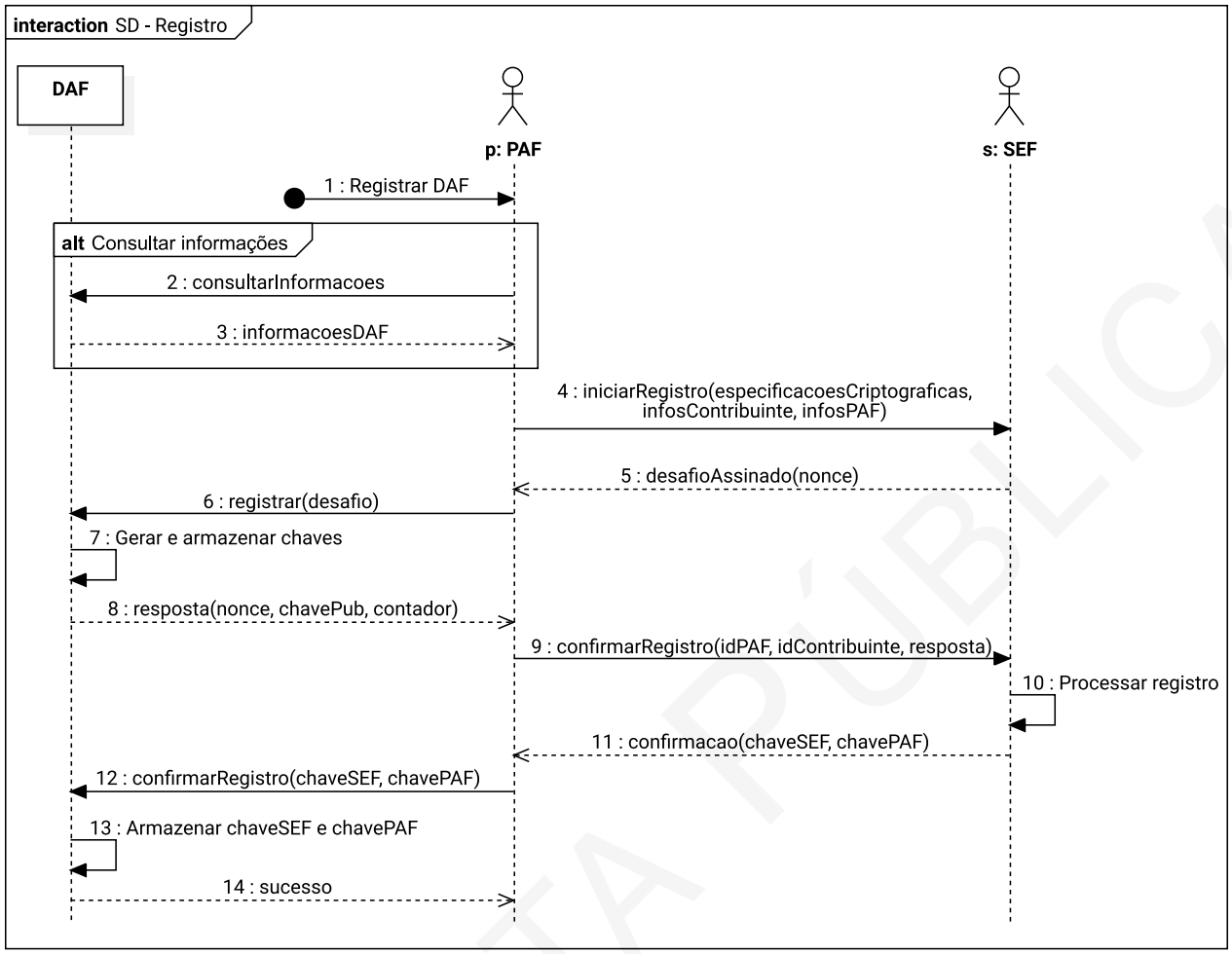
1. Contribuinte possui registro junto à SEF e possui e-CNPJ válido;
2. PAF possui registro junto à SEF e tem o Código de Segurança do Responsável Técnico (CSRT) (ENCAT, 2019c) associado a esse;
3. O desenvolvedor do PAF gerou um Identificador único do PAF (IdPAF) para o contribuinte;
   3.1. O IdPAF consiste na saída de uma função *hash* criptográfica HMAC-SHA256 (KRAWCZYK; BELLARE; CANETTI, 1997) que teve como chave o CSRT e como mensagem o CNPJ do contribuinte, representada em Base64URL (JOSEFSSON, 2006);
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;
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-4.6.

1. O registro é iniciado pelo contribuinte, o qual invoca rotina específica do PAF para registro de DAF;
2. O PAF solicita ao DAF informações sobre o DAF, buscando os algoritmos criptográficos que este é capaz de operar (Veja descrição da mensagem na Subseção 6.2.8);
3. O DAF retorna as informações solicitadas;
4. PAF envia à SEF pedido para registro de DAF (Veja descrição do serviço na Subseção 8.6.1)

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



4.1. Pedido contém detalhes sobre os algoritmos criptográficos que o DAF é capaz de operar, CNPJ do contribuinte e informações sobre o PAF, o que inclui o IdPAF daquele contribuinte, CNPJ do responsável técnico do PAF e o idCSRT que foi usado para gerar o IdPAF;

4.2. O pedido é assinado com o e-CNPJ do contribuinte.

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 Subseção 6.2.1);

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.

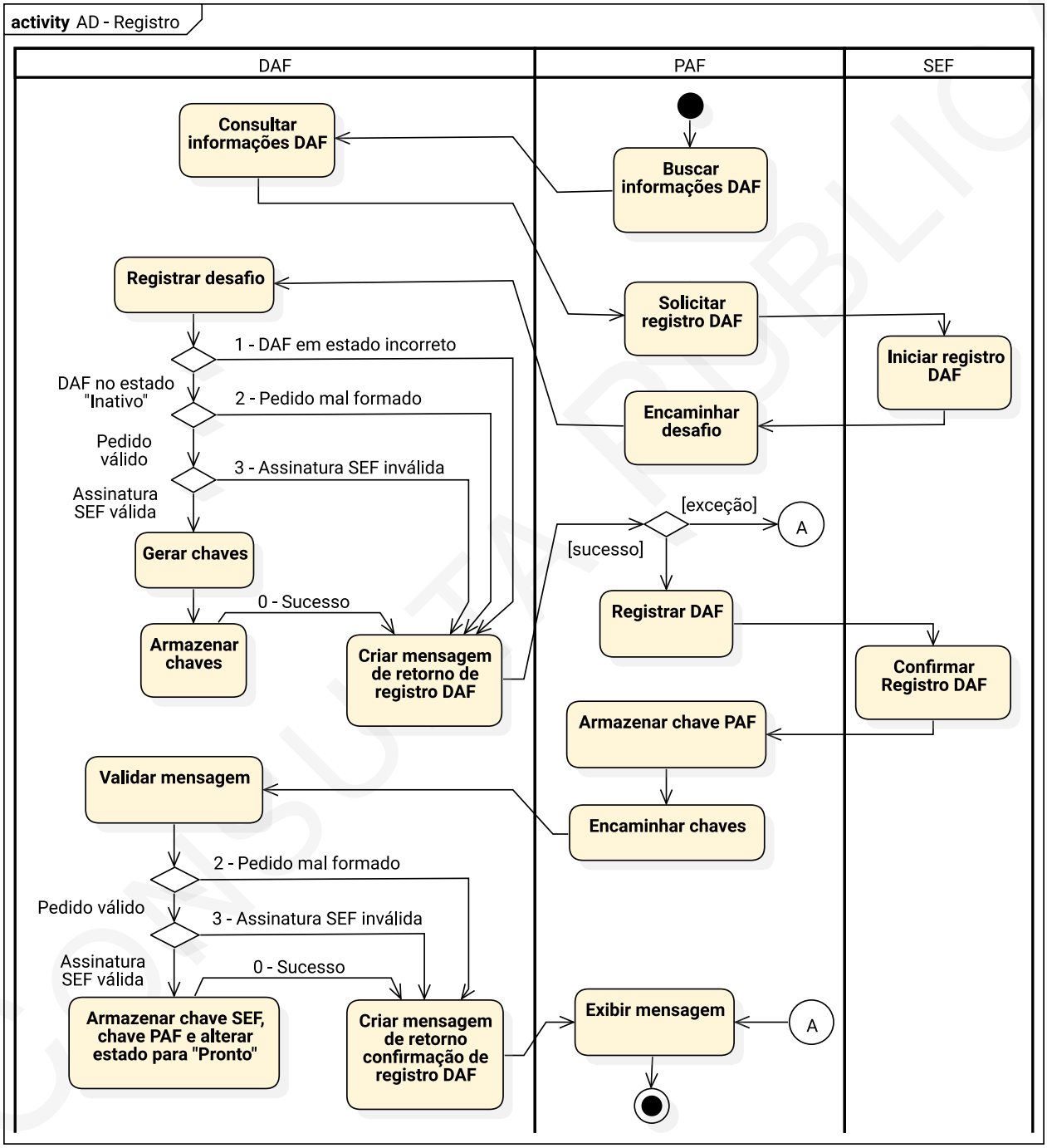
8. O DAF gera um documento contendo o atual valor de seu contador monotônico, o IdDAF, sua chave pública, e o *nonce* fornecido pela SEF. Esse documento é então assinado com sua chave privada e com a chave de ateste e encaminhado ao PAF;
9. O PAF encaminha a reposta do DAF à SEF juntamente com seu IdPAF e assina tudo isso com o e-CNPJ do contribuinte (Veja descrição do serviço na Subseção 8.6.2);
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, persiste o IdPAF, informações do contribuinte, o IdDAF, a chave pública do DAF, o identificador do modelo de 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; e a chave PAF. 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 Subseção 6.2.2);
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. 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.

Figura 5.2: Diagrama de atividade do processo de registro do DAF

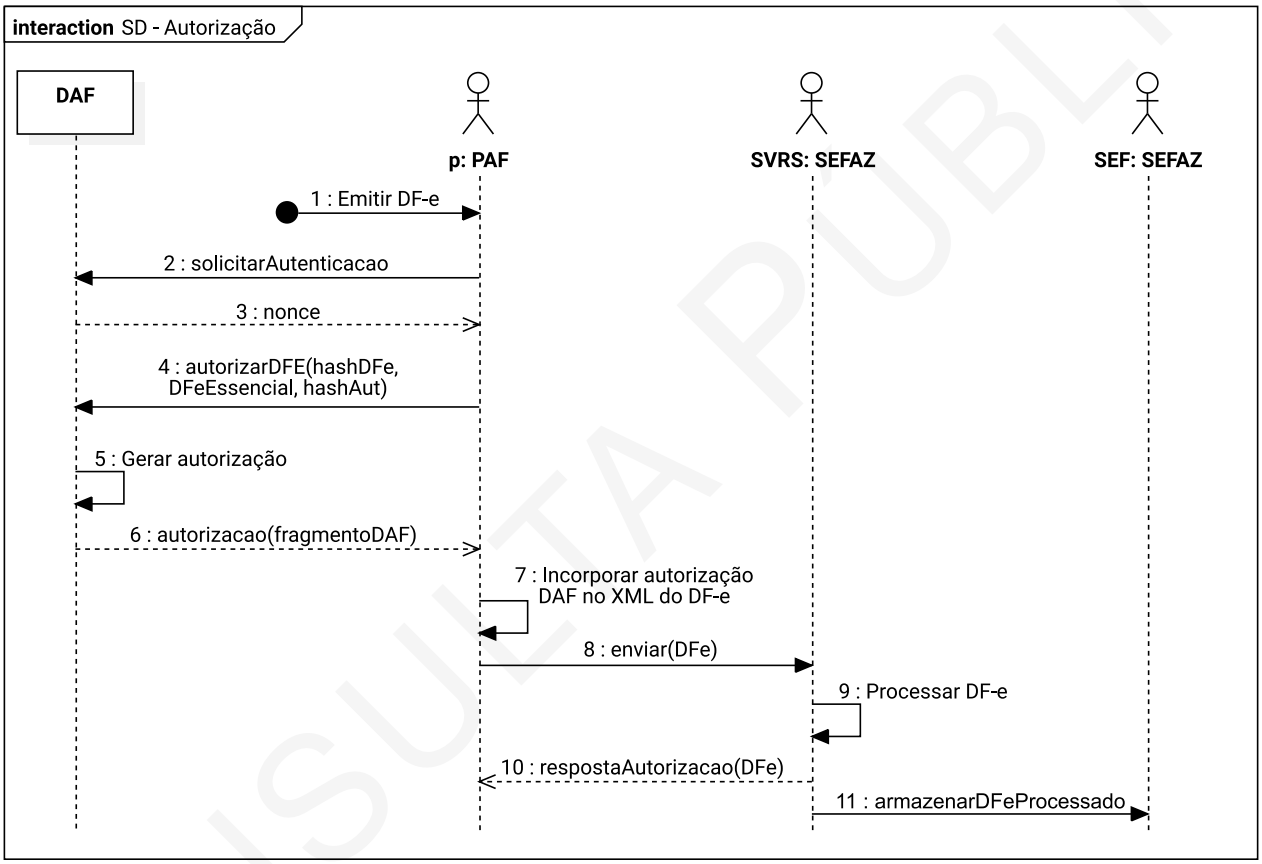


5.2 Autorização de Documentos Fiscais Eletrônicos (DF-e)

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 nos Casos de Uso UC-4.5 e UC-4.2.

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 Subseção 6.2.3);
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 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 Subseção 6.2.4);

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 atual valor de seu contador monotônico e o idAut, no caso a 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 o resumo criptográfico 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-4.2).
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, o que inclui verificar a 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 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	`infNFe`	Grupo raiz do documento com informações essenciais
2	A02	`versao`	Atributo de `infNFe` com a versão do leiaute da NFC-e
3	A03	`ID`	Atributo de `infNFe` com a chave de acesso da NFC-e
4	B01	`ide`	Grupo de informações de identificação da NFC-e
5	W01	`total`	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 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	`infBPe`	Grupo raiz do documento com informações essenciais
2	2	`versao`	Atributo de `infBPe` com a versão do leiaute do BP-e
3	3	`ID`	Atributo de `infBPe` com a chave de acesso do BP-e
4	4	`ide`	Grupo de informações de identificação do BP-e
5	125	`imp`	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 os espaços em branco usados somente 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 Seção 6.1). O *token* JWT DEVE ter sua integridade e autenticidade garantida por meio de uma função HMAC-SHA256 que teve como chave a chave SEF

(Veja Subseção 6.2.4).

5.2.3 Incorporação da autorização gerada pelo DAF nos DF-e

O PAF DEVE incorporar no DF-e a autorização gerada pelo DAF (Veja Subseção 5.2.2). O *token* JWT emitido pelo DAF DEVE ficar como valor do campo `infAdFisco`, previsto em (ENCAT, 2019a,b).

O campo `infAdFisco` está contido no grupo `infAdic`, que por sua vez é parte do grupo principal do DF-e, `infNFe` para NFC-e ou `infBPe` para BP-e. Deste modo, é necessário que o PAF o incorpore a autorização gerada pelo DAF antes de assinar o DF-e com o e-CNPJ do contribuinte. Na Listagem 5.1 é apresentado um exemplo com a autorização DAF incorporada no campo `infAdFisco` de uma NFC-e.

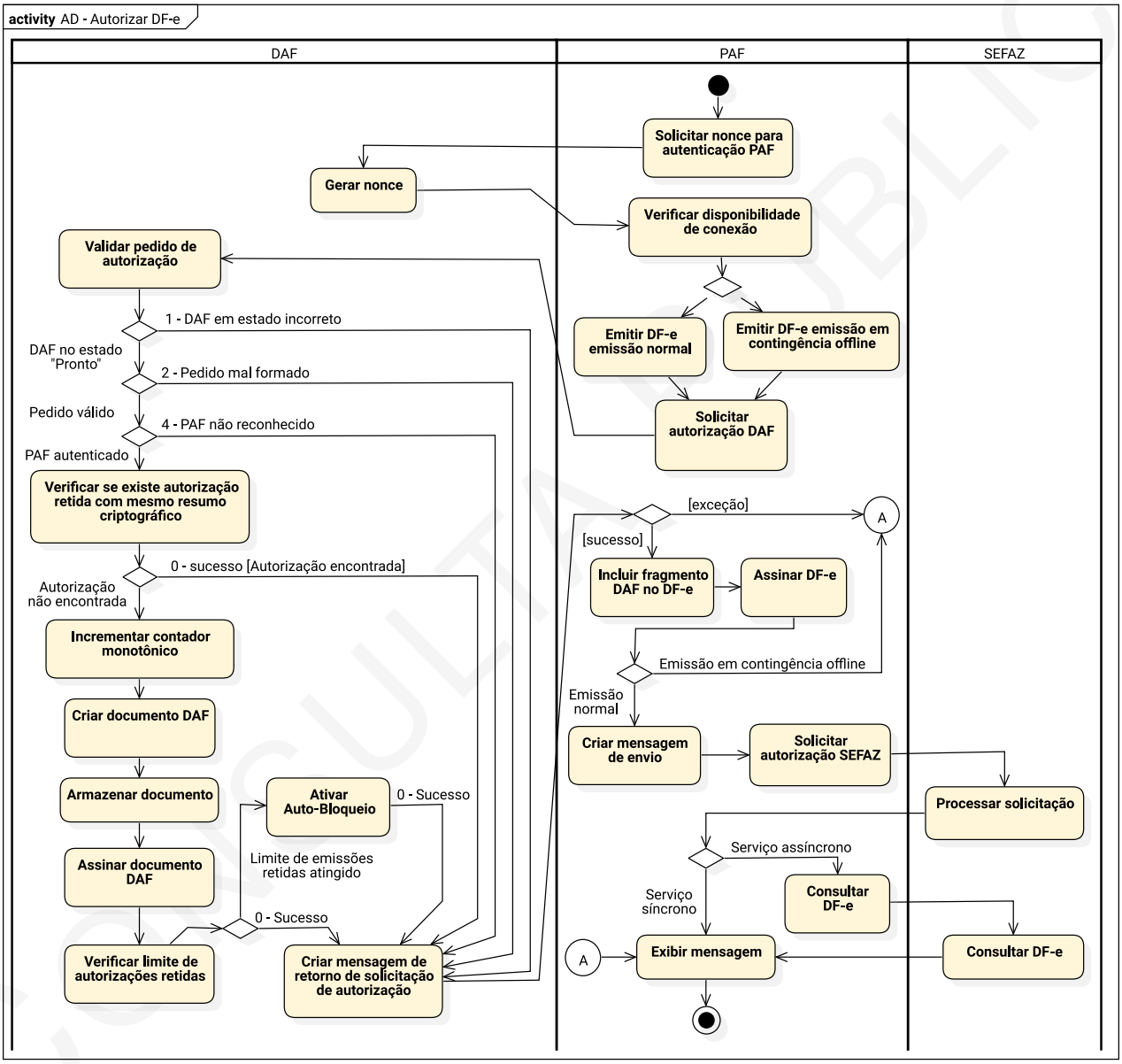
Listagem 5.1: Exemplo de NFC-e que contém a autorização gerada DAF

```
<NFe xmlns="http://www.portalfiscal.inf.br/nfe">
  <infNFe Id="NFe41200880249881000118650010000278531000123456" versao="4.00">
    <!-- Elementos suprimidos pra facilitar a visualização do exemplo-->
    <infAdic>
      <!-- Elementos suprimidos pra facilitar a visualização do exemplo-->
      <infAdFisco>
        eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJjb3VudCI6NDUsImlkQXV0IjoiaXZveURHTHFmMmhXX0cy
        bklRUjRXNzgyZmxDTDJ3OWpicUFhU3VaYmpLYyIsImlkREFGIjoiSWY0cXNzNUpsaFJMTHF5MXpfcWNFZyJ9.
        o7CkMI8uI5kMptR9CEjUKxCFXBxeJXAf8SJqpuzeXR8
      </infAdFisco>
    </infAdic>
  </infNFe>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><!-- Assinatura --></Signature>
</NFe>
```

5.2.4 Exceções

Durante o processo, o PAF é responsável pela comunicação com o DAF e a SEFAZ. Assim, caso um destes sistemas incorram em exceção, a mensagem será tratada pelo PAF. A Figura 5.4 ilustra o 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

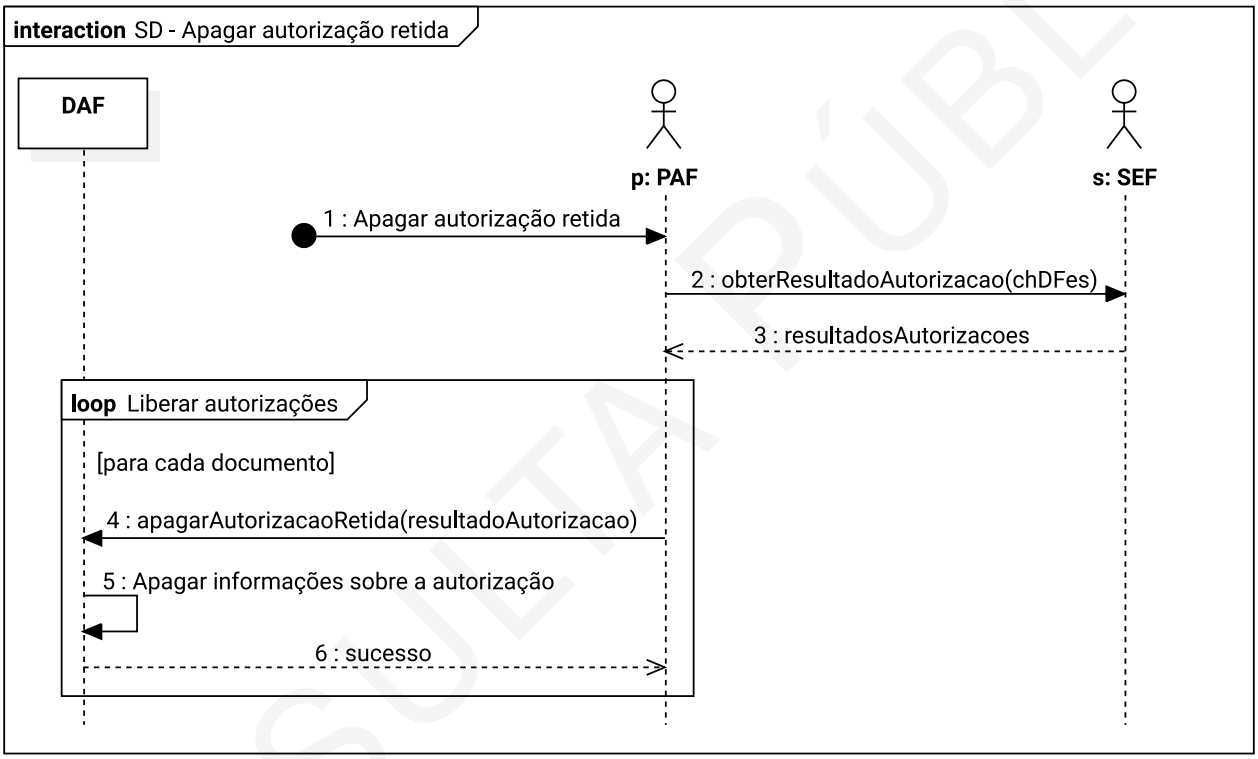


5.3 Apagar autorizações retidas no DAF

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-4.1.

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 cuja autorização está retida no DAF (Veja descrição do serviço na Subseção 8.10.1);
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 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. O PAF, para cada DF-e contido no documento recebido da SEF, encaminha ao DAF o idAut e a saída da função HMAC (Veja descrição da mensagem na Subseção 6.2.5);
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.

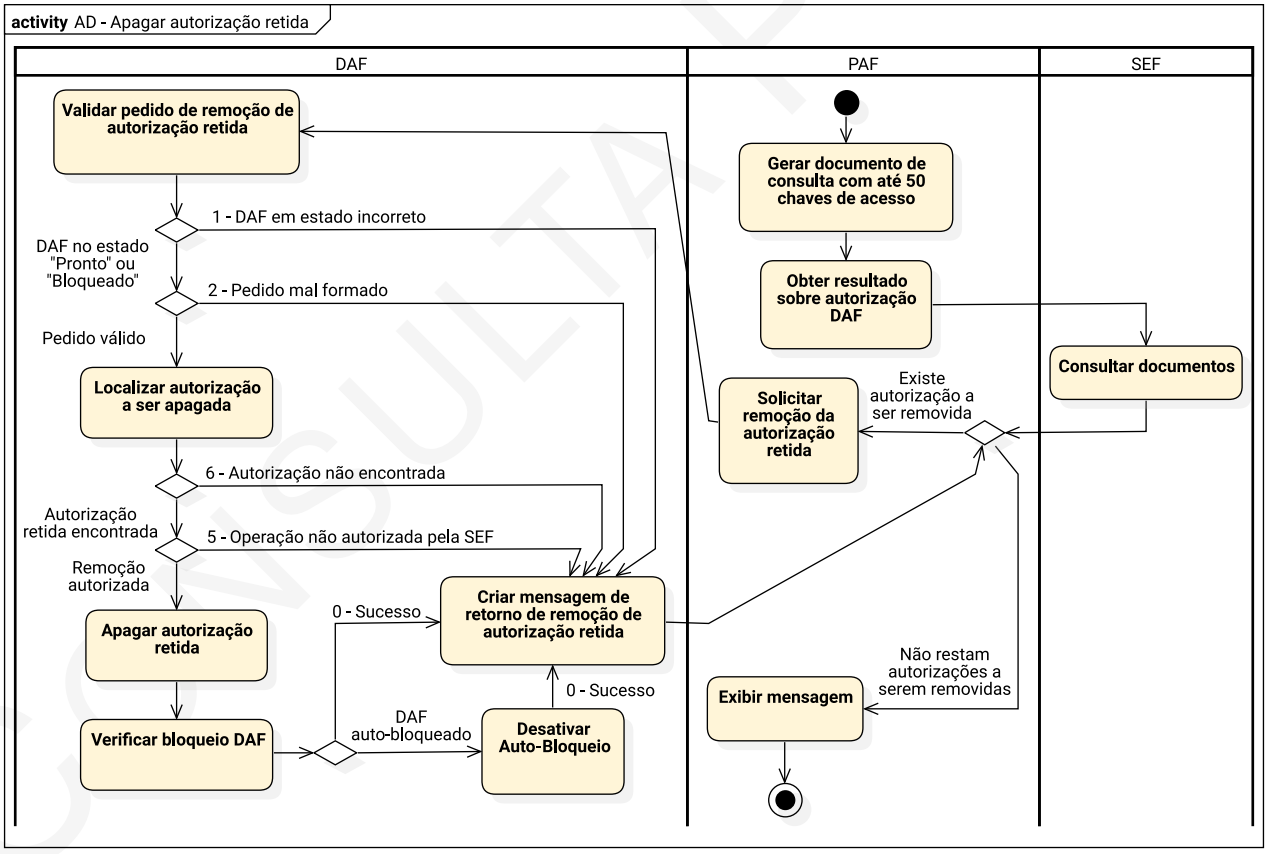
6. O DAF retorna a mensagem de sucesso ao PAF.

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 liberar autorizações retidas na MT.

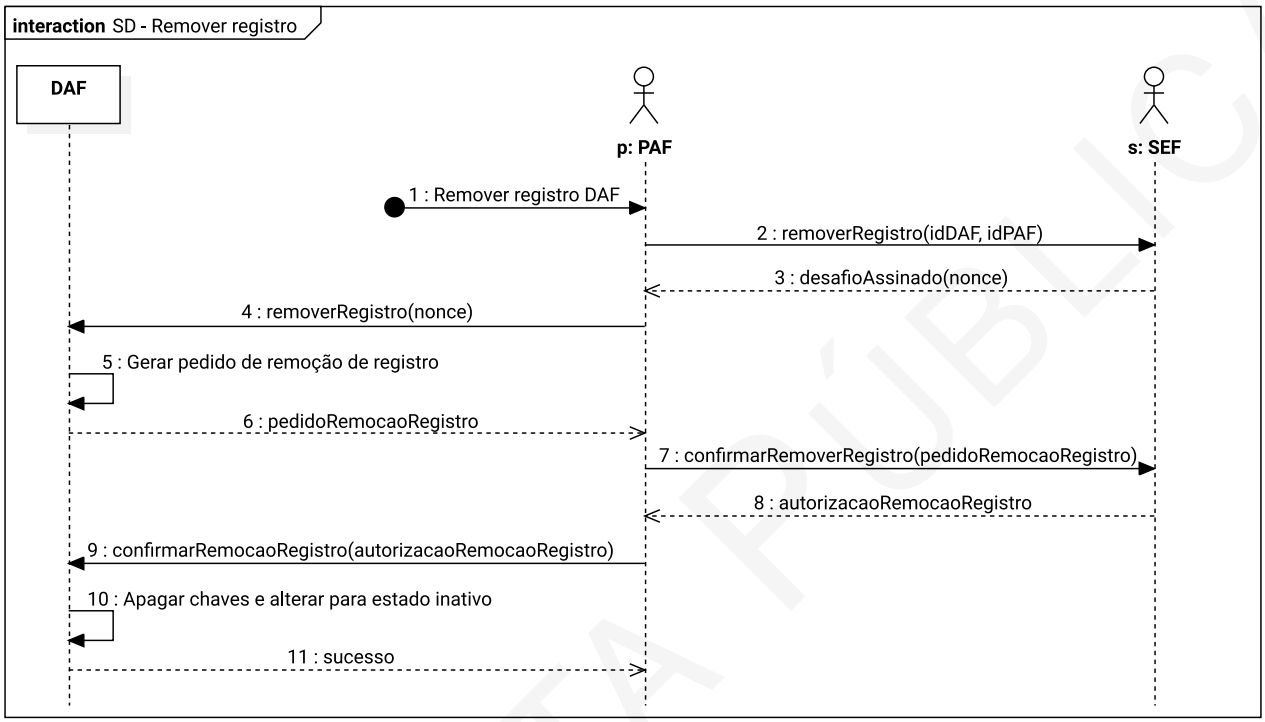
Figura 5.6: Diagrama de atividade do processo para apagar autorizações retidas



5.4 Remover registro do DAF junto à SEF

Na Figura 5.7 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-4.1.

Figura 5.7: 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 8.7.1);
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 Subseção 6.2.6);
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.

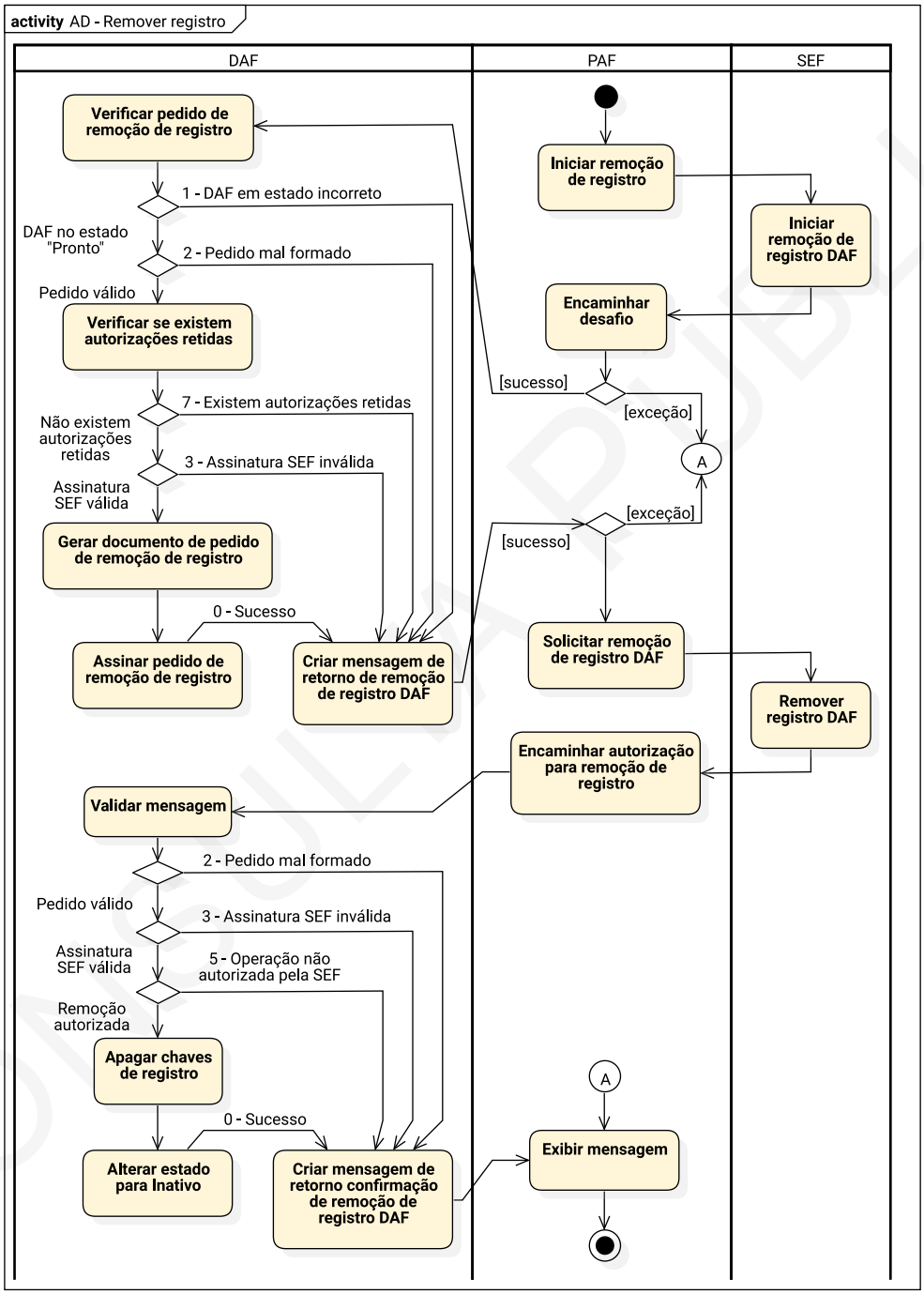
6. O DAF retorna para o PAF o documento gerado no passo anterior;
7. O PAF encaminha à SEF o documento gerado pelo DAF (Veja descrição do serviço na Subseção 8.7.2);
8. A SEF recebe o pedido de remoção de registro e:
   8.1. Verifica a correspondência do *nonce* e se a assinatura do documento gerada pela chave privada do DAF é válida;
   8.2. Remove o registro do DAF e gera um documento estruturado contendo a cadeia de caracteres `REMOVER`. 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 Subseção 6.2.7);
10. O DAF recebe o pedido e, em uma transação atômica:
    10.1. Verifica se o pedido foi formado adequadamente;
    10.2. Verifica se a assinatura da SEF sobre a mensagem é válida;
    10.3. Verifica se a cadeia de caracteres contida no documento corresponde a `REMOVER`;
    10.4. 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.

5.4.1 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 5.8 ilustra o diagrama de atividade UML, especificando as exceções possíveis no processo para remover o registro DAF.

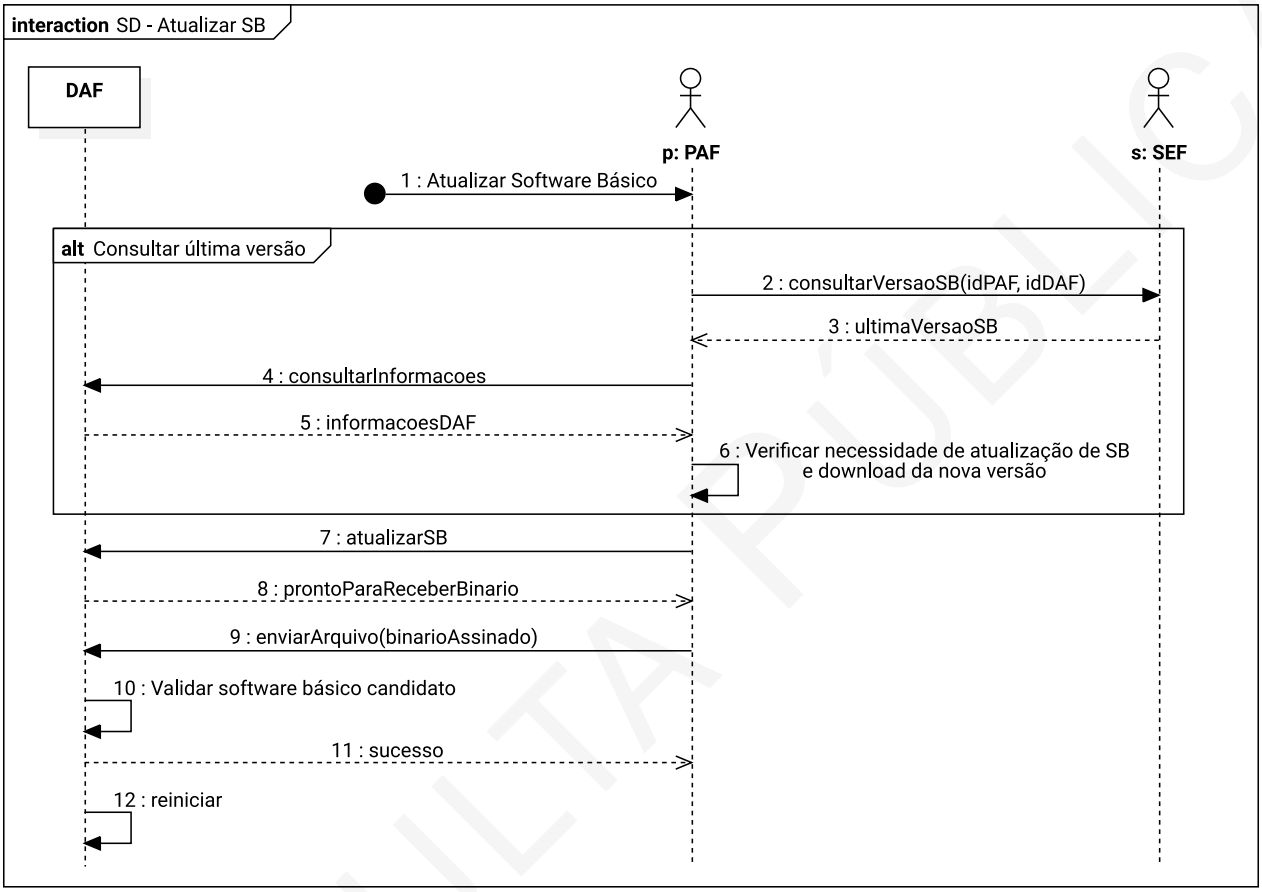
Figura 5.8: Diagrama de atividade do processo para remover o registro do DAF junto à SEF



5.5 Atualizar Software Básico

Na Figura 5.9 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-4.4 e UC-4.6.

Figura 5.9: 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 à SEF informações sobre a última versão de SB disponibilizada pelo fabricante do DAF, neste pedido devem constar o IdPAF e o IdDAF (Veja descrição do serviço na Subseção 8.8.1);
3. A SEF envia ao PAF um documento estruturado contendo a versão do último SB para o modelo de DAF correspondente ao IdDAF 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;
4. O PAF solicita ao DAF suas informações (Veja descrição da mensagem na Subseção 6.2.8);
5. O DAF retorna suas informações;
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

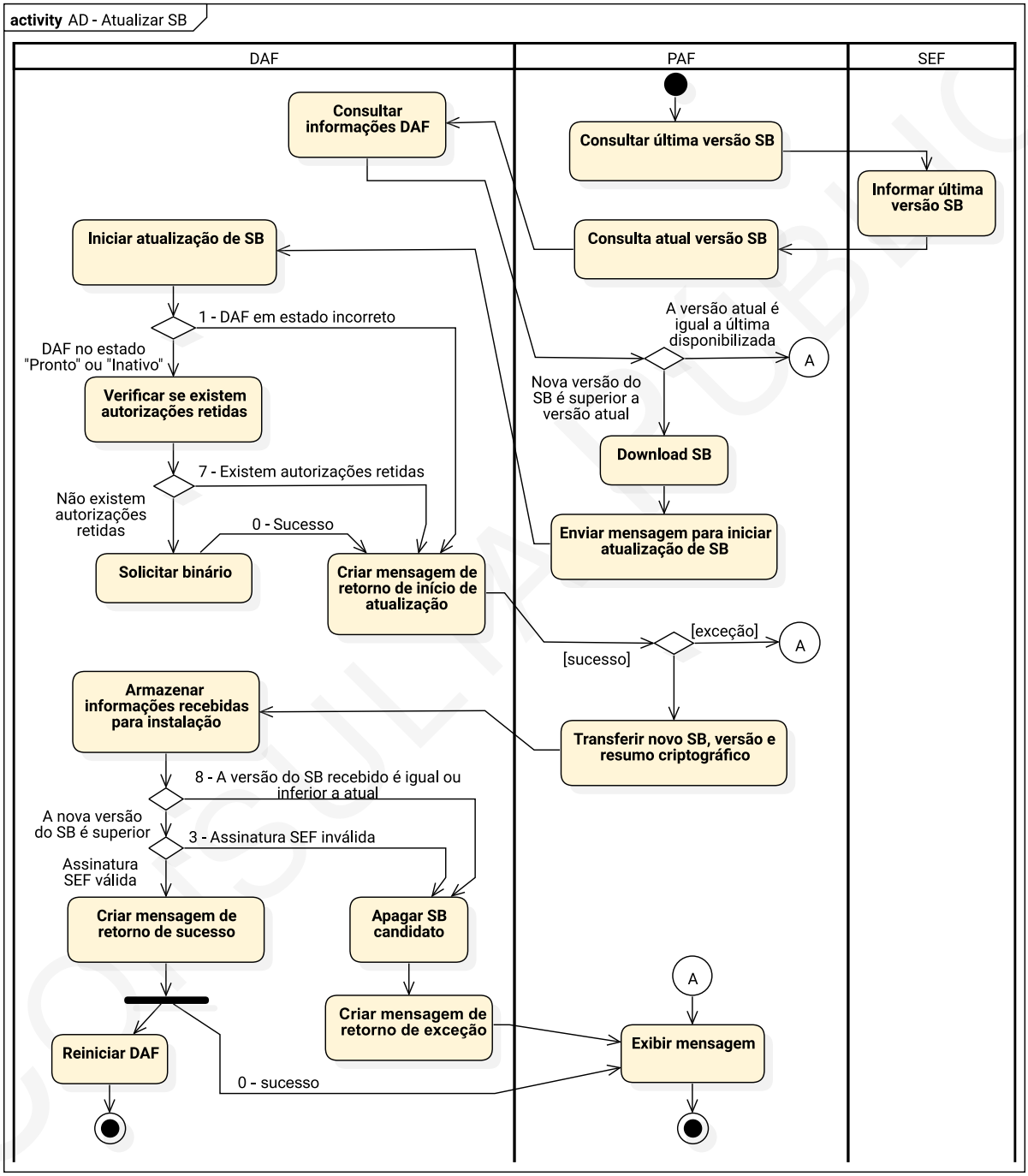
mensagem na Subseção 6.2.9);

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 Subsubseção 6.3.1.2);
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. O DAF informa ao PAF que o SB foi recebido com sucesso;
    11.4. O DAF é reiniciado automaticamente.

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 5.10 ilustra o diagrama de atividade UML, especificando as exceções possíveis no processo para atualizar o SB do o DAF.

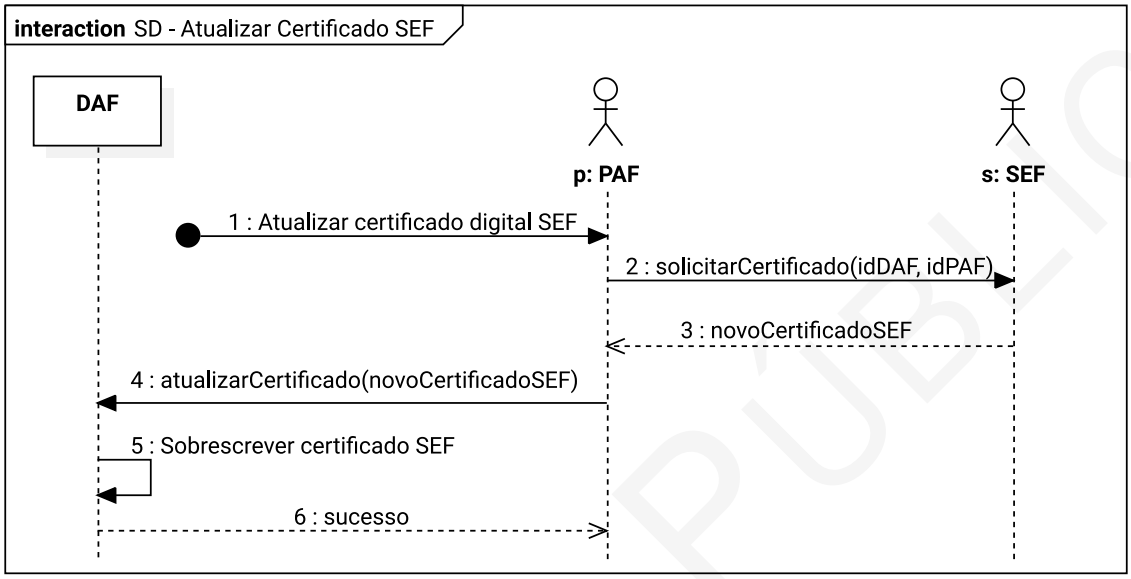
Figura 5.10: Diagrama de atividade do processo para atualizar o SB do DAF



5.6 Atualizar certificado digital SEF

Na Figura 5.11 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-4.3.

Figura 5.11: Diagrama de sequência do processo para atualizar o certificado digital SEF no DAF

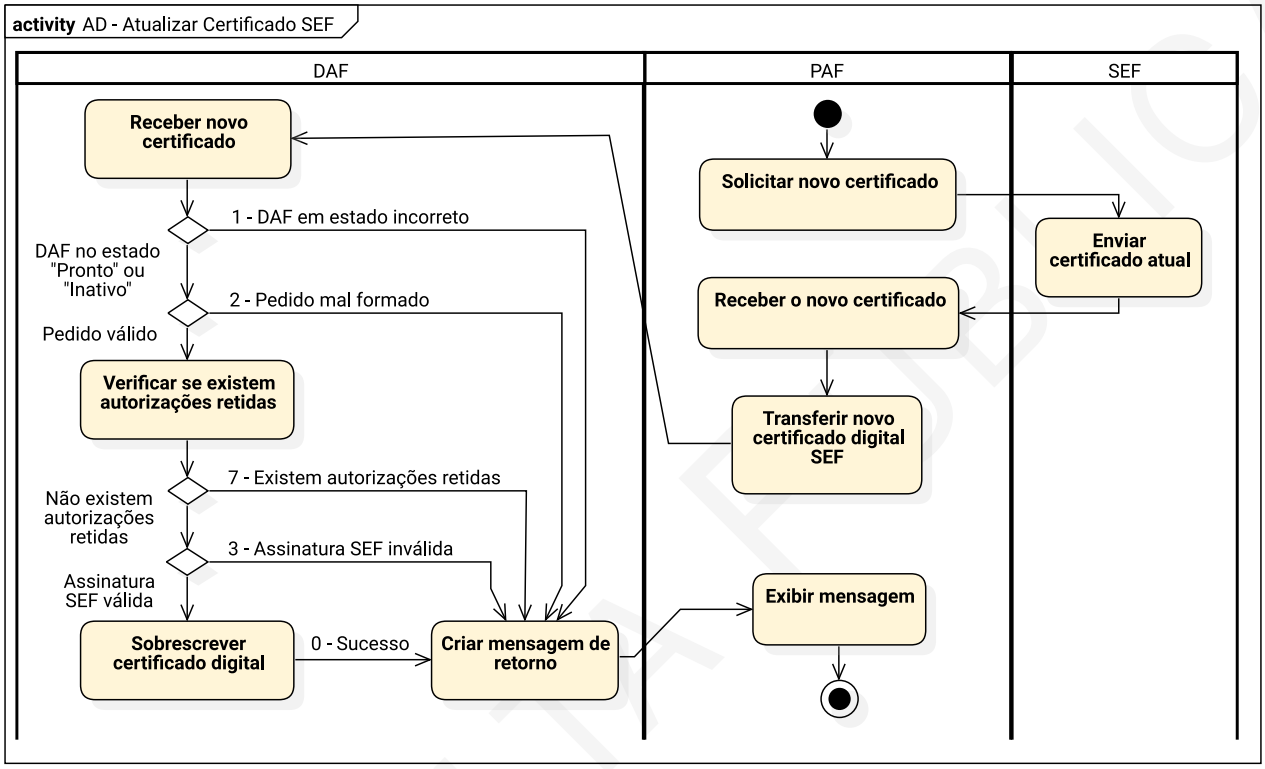


1. O processo é iniciado pelo contribuinte, o qual invoca a rotina específica do PAF para atualizar o certificado digital SEF armazenado no DAF;
2. O PAF solicita à SEF o atual certificado digital válido para o DAF que opera. No pedido são enviados o IdPAF e o IdDAF (Veja descrição do serviço na Subseção 8.9.1);
3. A SEF retorna um arquivo contendo o certificado digital codificado no formato textual PEM (JOSEFSSON; LEONARD, 2015);
4. O PAF transfere para o DAF o certificado digital recebido da SEF (Veja descrição da mensagem na Subseção 6.2.10);
5. O DAF recebe o novo certificado e, em uma transação atômica:
   5.1. Verifica se está no estado PRONTO ou INATIVO;
   5.2. Verifica se o pedido foi formado adequadamente;
   5.3. Verifica se possui autorizações retidas em sua MT;
   5.4. 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;
   5.5. Sobrescreve certificado digital da SEF.
6. O DAF retorna uma mensagem de sucesso ao PAF, que por sua vez informa ao usuário;

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 5.12 ilustra o diagrama de atividade UML, especificando as exceções possíveis no processo para atualizar o certificado SEF armazenado no DAF.

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



6 Protocolo de comunicação

O DAF consiste de um dispositivo passivo que só reage mediante a um estímulo do PAF. Sendo assim, o protocolo de comunicação do DAF está fundamentado sobre o modelo de pedido e resposta, ou seja, um comando consiste em um pedido seguido por uma resposta e cada comando deve ser realizado de forma atômica. Sendo assim, o DAF NÃO DEVE ser interrompido enquanto processa o pedido de um comando. Neste capítulo as seguintes definições são feitas:

- **Mensagem**: as mensagens definidas na Seção 6.2, utilizadas para que o PAF e o DAF possam implementar os casos de uso e processos operacionais apresentados na Capítulo 4 e na Capítulo 5. Cada mensagem DEVE ter um pedido e uma resposta e sua representação é definida na Seção 6.1;
- **Comandos**: os comandos transportam as mensagens apresentadas na Seção 6.2, além de serem utilizados para outras funções de comunicação entre o PAF e o DAF. Cada comando é composto de um pedido e uma resposta.

6.1 Representação das mensagens da API DAF

O conjunto de mensagens 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, toda mensagem recebida pelo DAF receberá uma resposta assim que o DAF terminar seu processamento.

Para que o DAF possa atender seu propósito, as mensagens DEVEM ser trocadas de acordo com os casos de uso apresentados na Seção 4.1 e os processos apresentados no Capítulo 5. Os pedidos e respostas referentes a cada mensagem da API (Veja Seção 6.2) do DAF devem representados de acordo com as seguintes regras:

1. Os pedidos e respostas referentes às mensagens 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 da mensagem ou o código da resposta (Veja Tabela 6.1 e Tabela 6.2) DEVEM aparecer

como o primeiro par de chave e valor no documento JSON. Para a mensagem 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 Seção 6.2 (Veja exemplo de representação de pedido e resposta de mensagem 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 de mensagens assinadas 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 informacões sobre o algoritmo criptográfico utilizado para gerar a assinatura do *token*;
      4.2.1. Para mensagens 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` e de acordo com a especificação *JSON Web Key* (JWK) (JONES, 2015);
      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 Seção 6.2;
      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 operações:
   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.

6.2 Mensagens da API DAF

Na Tabela 6.1 estão listados as mensagens com seus códigos, indicação se a mensagem possui parâmetros, o tipo de resposta que será retornada e em quais casos de uso as mensagens poderão ser usadas. O tipo de resposta poderá ser:

- **completa** – quando a resposta da mensagens exigir além do código da resposta, outros parâmetros; ou
- **apenas código** – quando a resposta da mensagem não exigir parâmetros extras.

Algumas mensagens da API DAF são referentes ao mesmo caso de uso. Para as mensagens desse cenário, as regras abaixo se aplicam:

1. O DAF DEVE abortar a execução do caso de uso se não receber a próxima mensagem esperada em no máximo 120 segundos.

Tabela 6.1: Mensagens da API DAF

Nome da mensagem	Código	Parâmetros	Tipo de resposta	Caso de uso
`registrar`	1	sim	completa	UC-4.10
`confirmarRegistro`	2	sim	apenas código	UC-4.10
`solicitarAutenticacao`	3	não	completa	UC-4.5
`autorizarDFE`	4	sim	completa	UC-4.5
`apagarAutorizacaoRetida`	5	sim	apenas código	UC-4.1
`removerRegistro`	6	sim	completa	UC-4.11
`confirmarRemocaoRegistro`	7	sim	apenas código	UC-4.11
`consultarInformacoes`	8	não	completa	UC-4.6
`atualizarSB`	9	não	apenas código	UC-4.4
`atualizarCertificado`	10	sim	apenas código	UC-4.3
`descarregarRetidos`	11	sim	completa	UC-4.8
`cancelarProcesso`	12	não	apenas código	-

Na Tabela 6.2 são listadas as respostas que poderão ser geradas pelo DAF, juntamente com seus os códigos e descrições.

Tabela 6.2: Códigos das respostas às mensagens

Nome da resposta	Valor	Descrição
`sucesso`	0	Sucesso no processamento da mensagem anterior
`estadoIncorreto`	1	DAF em estado incorreto
`pedidoMalFormado`	2	Pedido formado de forma inadequada
`assinaturaInvalida`	3	Assinatura SEF inválida
`pafDesconhecido`	4	PAF não reconhecido pelo DAF
`operacaoNaoAutorizada`	5	Operação não autorizada pela SEF

`autorizacaoNaoEncontrada`	6	Autorização não encontrada na MT do DAF
`autorizacaoRetida`	7	DAF com autorizações retidas
`versaoSBInvalida`	8	Versão do SB inferior ou igual à versão existente

A listagem Listagem 6.1 apresenta um exemplo genérico de como uma resposta do tipo **apenas código** DEVE ser representada, na qual o valor da chave `res` DEVE ser um dos códigos de resposta apresentados na Tabela 6.2, de acordo com a situação.

Listagem 6.1: Documento JSON para resposta do tipo “apenas código”

```
{
    "res": 0
}
```

Nas subseções a seguir são apresentados os detalhes sobre o pedido e resposta para cada mensagem.

6.2.1 `registrar`

Essa mensagem é enviada 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 Seção 6.1);
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 Seção 6.1);
   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 informacões 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.

6.2.2 `confirmarRegistro`

Essa mensagem é enviada 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).

Tabela 6.3: Informações encaminhadas no pedido da mensagem `registrar`

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
`nonce`	22	*string*	Valor aleatório gerado pela SEF representado em Base64URL

Tabela 6.4: Informações encaminhadas na resposta da mensagem `registrar`

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
`idDAF`	22	*string*	Identificador único do DAF representado em Base64URL
`cont`	4	inteiro	Valor atual do contador monotônico
`nonce`	22	*string*	Valor aleatório gerado pela SEF representado em Base64URL

1. O documento JSON do pedido DEVE conter apenas duas chaves: `msg`, associada ao valor `2`, e `jwt` (Veja Seção 6.1);
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.
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 6.5: Informações encaminhadas no pedido da mensagem `confirmarRegistro`

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
`chSEF`	variável	*string*	Chave SEF cifrada com a chave pública do DAF, com o esquema de cifragem `RSAES-OAEP` (MORIARTY et al., 2016), e representada em Base64URL
`chPAF`	86	*string*	Chave PAF representada em Base64URL

6.2.3 `solicitarAutenticacao`

Essa mensagem é enviada pelo PAF para receber um *nonce* gerado pelo DAF (Veja o Caso de Uso UC-4.5 e o processo descrito na Seção 5.2).

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)`. A Tabela 6.2 apresenta a descrição desse erro.

Tabela 6.6: Informações encaminhadas na resposta da mensagem `solicitarAutenticacao`

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
`nonce`	22	*string*	Valor aleatório gerado pelo DAF representado em Base64URL

6.2.4 `autorizarDFE`

Essa mensagem é enviada pelo PAF para solicitar autorização sobre um DF-e (Veja o Caso de Uso UC-4.5 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 da mensagem `autorizarDFE`

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
`fragDFE`	variável	*string*	Documento XML com as informações essenciais do DF-e codificado em Base64URL
`hashDFE`	43	*string*	Resumo criptográfico do DF-e completo representado em Base64URL
`respDes`	43	*string*	Saída de uma função HMAC representada em Base64URL (veja Caso de Uso UC-4.5)

Tabela 6.8: Informações encaminhadas na resposta da mensagem `autorizarDFE`

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
`idDAF`	22	*string*	Identificador único do DAF representado em Base64URL
`cont`	4	inteiro	Valor atual do contador monotônico
`versaoSB`	variável	*string*	Versão atual do software básico
`idAut`	43	*string*	Identificador único da autorização DAF representado em Base64URL

6.2.5 `apagarAutorizacaoRetida`

Essa mensagem é enviada pelo PAF para remover uma autorização retida na na MT do DAF (Veja o Caso de Uso UC-4.1 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)`, `operacaoNaoAutorizada (5)` ou `autorizacaoNaoEncontrada (6)`. As descrições das respostas de erro podem ser encontradas na Tabela 6.2.

Tabela 6.9: Informações encaminhadas no pedido da mensagem `apagarAutorizacaoRetida`

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
`idAut`	43	*string*	Identificador único da autorização DAF representado em Base64URL
`autApag`	43	*string*	Saída de uma função HMAC representada em Base64URL que teve como chave a chave SEF e como mensagem o idAut

6.2.6 `removerRegistro`

Essa mensagem é enviada 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 5.4).

1. O documento JSON do pedido DEVE conter apenas duas chaves: `msg`, associada ao valor `6`, e `jwt` (Veja Seção 6.1);
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 da mensagem `removerRegistro`

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
`nonce`	22	*string*	Valor aleatório gerado pela SEF representado em Base64URL

Tabela 6.11: Informações encaminhadas na resposta da mensagem `removerRegistro`

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
`idDAF`	22	*string*	Identificador único do DAF representado em Base64URL
`cont`	4	inteiro	Valor atual do contador monotônico
`nonce`	22	*string*	Valor aleatório gerado pela SEF representado em Base64URL

6.2.7 `confirmarRemocaoRegistro`

Essa mensagem é enviada pelo PAF para finalizar o processo de remoção de registro do DAF junto a SEF que fora previamente inciado (Veja o Caso de Uso UC-4.11 e o processo descrito na Seção 5.4).

1. O documento JSON do pedido DEVE conter apenas duas chaves: `msg`, associada ao valor `7`, e `jwt` (Veja Seção 6.1);
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)`, `assinaturaInvalida (3)` ou `operacaoNaoAutorizada (5)`. As descrições das respostas de erro podem ser encontradas na Tabela 6.2.

Tabela 6.12: Informações encaminhadas no pedido da mensagem `confirmarRemocaoRegistro`

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
`evento`	7	*string*	Cadeia de caracteres `REMOVER`

6.2.8 `consultarInformacoes`

Essa mensagem é enviada pelo PAF ou pelo Aplicativo Fisco para obter informações sobre o DAF (Veja o Caso de Uso UC-4.6).

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;
   2.1. No vetor associado à chave `algos`, o DAF DEVE inserir um ou mais objetos JSON com as informações presentes na Tabela 6.14;
   2.2. O valor associado a chave `alg` DEVE ser representado como uma cadeia de caracteres conforme aparece no *alg Header Parameter* no capítulo 3 da RFC 7518 (JONES, 2018), respeitando o tipo chave criptográfica e algoritmo para gerar resumos criptográficos que o DAF provê suporte (Veja Subseção 2.4.1);
   2.3. O valor associado a chave `len` DEVE estar de acordo com o tamanho da chave criptográfica que o DAF provê suporte (Veja Subseção 2.4.1).
3. Em caso de insucesso, o DAF DEVE gerar uma resposta de `estadoIncorreto (1)`. A Tabela 6.2 apresenta a descrição desse erro.

6.2.9 `atualizarSB`

Essa mensagem é enviada pelo PAF para que o DAF se prepare para iniciar o processo de atualização de SB (Veja o Caso de Uso UC-4.4 e o processo descrito na Seção 5.5).

Tabela 6.13: Informações encaminhadas na resposta da mensagem `consultarInformacoes`

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
`idDAF`	22	*string*	Identificador único do DAF representado em Base64URL
`versaoSB`	variável	*string*	Versão atual do software básico
`hashSB`	43	*string*	Resumo criptográfico do software básico representado em Base64URL
`modelo`	variável	*string*	Modelo do DAF
`cont`	4	inteiro	Valor atual do contador monotônico
`cert`	variável	*string*	Certificado digital da SEF codificado no formato textual PEM de acordo com Josefsson e Leonard (2015)
`estado`	variável	*string*	Estado atual do DAF
`retidas`	variável	*array*	Vetor com Identificadores únicos das autorizações
`algos`	variável	*array*	Vetor com objetos JSON para indicar os algoritmos criptográficos que o DAF provê suporte

Tabela 6.14: Informações encaminhadas na chave `algos` da resposta da mensagem `consultarInformacoes`

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
`alg`	variável	*string*	Algoritmo criptográfico
`len`	2	inteiro	Tamanho da chave criptográfica

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)` ou `autorizacaoRetida (7)`. As descrições das respostas de erro podem ser encontradas na Tabela 6.2.

6.2.10 `atualizarCertificado`

Essa mensagem é enviada pelo PAF para atualizar o certificado digital da SEF armazenado no DAF (Veja o Caso de Uso UC-4.3 e o processo descrito na Seção 5.6).

1. O documento JSON do pedido DEVE conter a chave `msg`, associada ao valor `10`, e lista de parâmetros conforme apresentado na Tabela 6.15;
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.

6.2.11 `descarregarRetidos`

Essa mensagem é enviada pelo PAF ou pelo aplicativo fisco para que o DAF descarregue as autorizações retidas em sua MT (Veja o Caso de Uso UC-4.8).

Tabela 6.15: Informações encaminhadas no pedido da mensagem `atualizarCertificado`

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
`cert`	variável	*string*	Certificado digital da SEF codificado no formato textual PEM de acordo com Josefsson e Leonard (2015)

1. O documento JSON do pedido DEVE conter a chave `msg`, associada ao valor `11`, e lista de parâmetros conforme apresentado na Tabela 6.16;
2. Em caso de sucesso, o DAF DEVE gerar uma resposta de `sucesso (0)` com os parâmetros apresentados na Tabela 6.17;
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 6.16: Informações encaminhadas no pedido da mensagem `descarregarRetidos`

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
`idAut`	43	*string*	Identificador único da autorização DAF representado em Base64URL

Tabela 6.17: Informações encaminhadas na resposta da mensagem `descarregarRetidos`

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
`idAut`	43	*string*	Identificador único da autorização DAF representado em Base64URL
`fragDFE`	variável	*string*	Documento XML com as informações essenciais do DF-e codificado em Base64URL

6.2.12 `cancelarProcesso`

Essa mensagem é enviada pelo PAF para que o DAF cancele qualquer processo ou caso de uso que ele iniciara previamente.

1. O pedido não possui parâmetros e o documento JSON do pedido DEVE conter apenas a chave `msg` associada ao valor `12`;
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.

6.3 Características específicas do USB

A interface USB do DAF DEVE ser composta pela classe USB-CDC e pela subclasse *Abstract Control Model* (ACM) conforme (USB-IF, 2010) e (USB-IF, 2007), assim constituindo-se de uma porta serial virtual sobre a interface USB.

1. A velocidade do barramento DEVE respeitar a especificação apresentada na Seção 3.7;

2. O campo *iProduct* do *device descriptor* da interface USB do DAF DEVE conter um índice referente a um *string descriptor* cujo valor seja: "DAF-SC".

6.3.1 Comandos PDAF-CDC

Na Tabela 6.18 são apresentados os comandos para transportar, sobre o CDC, as mensagens entre DAF e PAF.

Tabela 6.18: Comandos de transporte

Nome do comando	Valor	Descrição
`enviarMensagem`	`0x01`	Envia uma mensagem em formato de representação JSON para a outra extremidade
`enviarBinario`	`0x02`	Envia dados brutos (*raw data*) para a outra extremidade
`ping`	`0x04`	Envia uma mensagem que será ecoada pela outra extremidade do barramento
`erro`	`0x05`	Uma operação não foi completada com sucesso

1. Na Tabela 6.19 é apresentada a estrutura do enquadramento de mensagens para o transporte CDC.
   1.1. No campo Comando DEVE ser informado um dos valores de comando apresentados na Tabela 6.18;
   1.2. O campo Tamanho DEVE possuir no mínimo 1 *byte* e no máximo 4 *bytes* de tamanho, respeitando os requisitos de cada comando;
   1.3. O campo Dados DEVE conter um pedido ou uma resposta da API DAF ou dados brutos (*raw data*) (Veja Seção 6.2).

Tabela 6.19: Estrutura do encapsulamento

Nome do campo	Ocorrência	Tamanho (*bytes*)	Descrição
Comando	1-1	1	Código do comando para a mensagem, conforme Tabela 6.18
Tamanho	1-1	variável	Tamanho do campo Dados, *byte* mais significativo enviado primeiro (*big-endian*)
Dados	1-1	variável	Dados que devem ser transmitidos para a outra extremidade do barramento

6.3.1.1 `enviarMensagem`

Este comando DEVE ser utilizado para o transporte de todas as mensagens apresentadas na API DAF (veja Seção 6.2).

1. O campo Tamanho DEVE possuir 2 *bytes*;
2. O campo Dados DEVE conter um pedido ou um resposta de uma mensagem da API DAF;
3. Em caso de sucesso, a resposta DEVE ser do tipo `enviarMensagem`;
4. Em caso de insucesso, a resposta DEVE ser do tipo `erro`.

6.3.1.2 `enviarBinario`

Este comando DEVE ser utilizado pelo PAF a fim de realizar a transferência de dados brutos (*raw data*), por exemplo, o arquivo contendo a imagem de atualização do SB (veja Caso de Uso UC-4.4).

1. O campo Tamanho DEVE possuir 4 *bytes*;
2. O campo Dados DEVE conter dados brutos (*raw data*);
3. Em caso de sucesso, a resposta DEVE ser do tipo `enviarMensagem`;
4. Em caso de insucesso, a resposta DEVE ser do tipo `erro`.

6.3.1.3 `ping`

Este comando PODE ser utilizado pelo PAF e é definido a fim de ser utilizado para depuração, verificação de latência e medições de desempenho da interface de comunicação entre o PAF e o DAF.

1. O campo Tamanho DEVE possuir 2 *bytes*;
2. O campo Dados DEVE conter dados arbitrários;
3. Em caso de sucesso, a resposta DEVE ser do tipo `ping`;
   3.1. O campo Dados DEVE conter os mesmos dados enviados no pedido.
4. Em caso de insucesso, a resposta DEVE ser do tipo `erro`.

6.3.1.4 `erro`

Este comando representa a ocorrência de um erro durante a validação de um comando do transporte CDC, podendo ser utilizado pelo PAF ou DAF.

1. O campo Tamanho DEVE possuir 1 *byte* e conter o valor `0x01`;
2. O campo Dados DEVE conter um dos códigos de erro apresentados na Tabela 6.20.

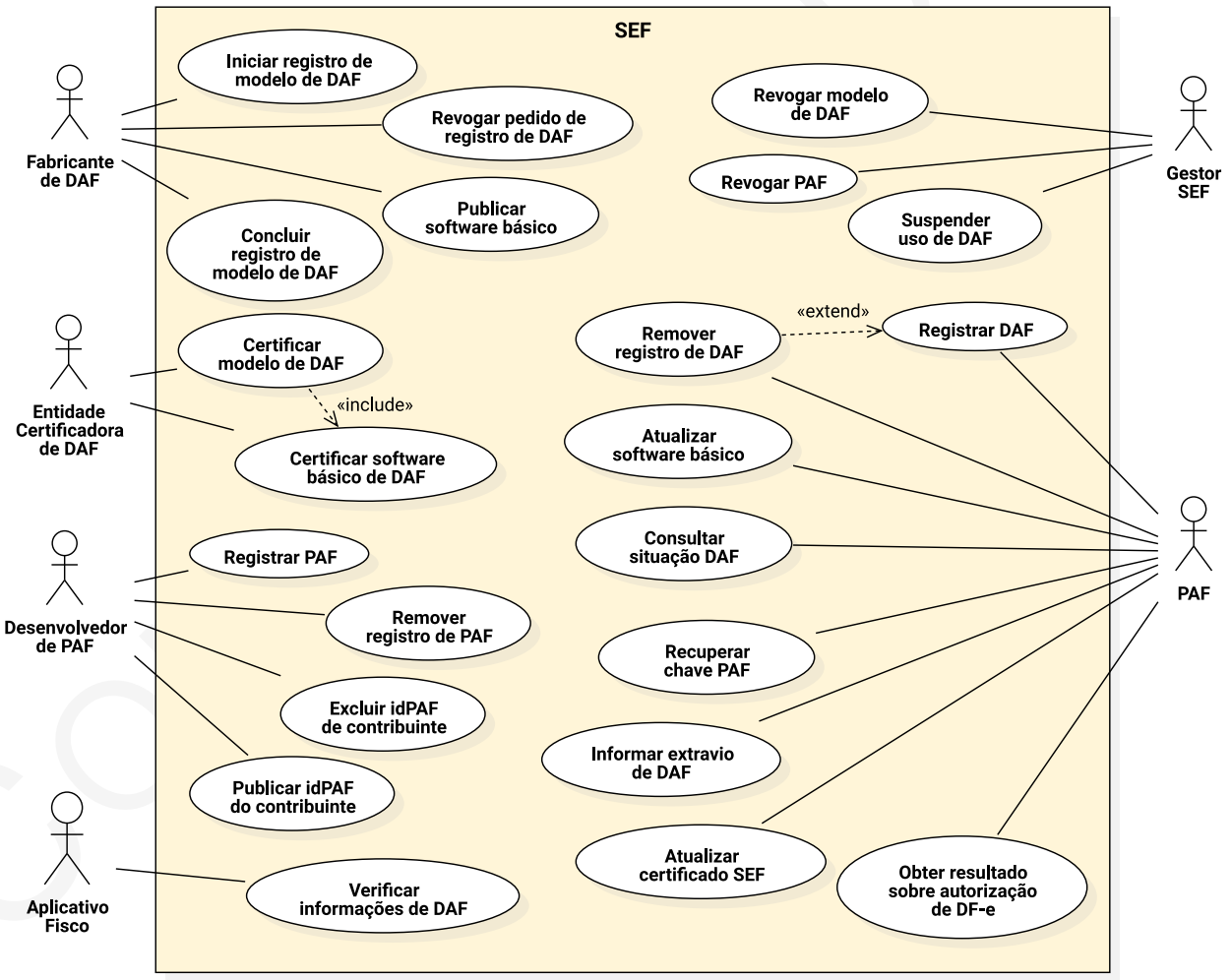
Tabela 6.20: Códigos de erro para o transporte DAF

Nome do comando	Valor	Descrição
`erroComandoInvalido`	`0x01`	O comando da requisição é inválido
`erroTamanhoInvalido`	`0x02`	O `Tamanho` informado não corresponde ao tamanho do campo `Dados`
`erroTimeout`	`0x03`	Tempo de espera esgotado
`erroDesconhecido`	`0x04`	Origem do erro não definida

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.

> O processo de emissão de certificado digital pela SEF, aqui descrito, tem com 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).

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, esse 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 e informações do contribuinte que está fazendo o registro. 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, sendo cada um operado pelo seu próprio PAF, conforme determinação do GESAC. Sendo assim, a SEF deve manter diversas bases, sendo essas:

1. Modelos de DAF certificados – detalhes sobre o fabricante, detalhes sobre a certificação, características criptográficas, chave pública par da chave de ateste, histórico de versões do 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 e o último valor conhecido do contador monotônico daquele 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 e IdDAF. 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 5.4).

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.

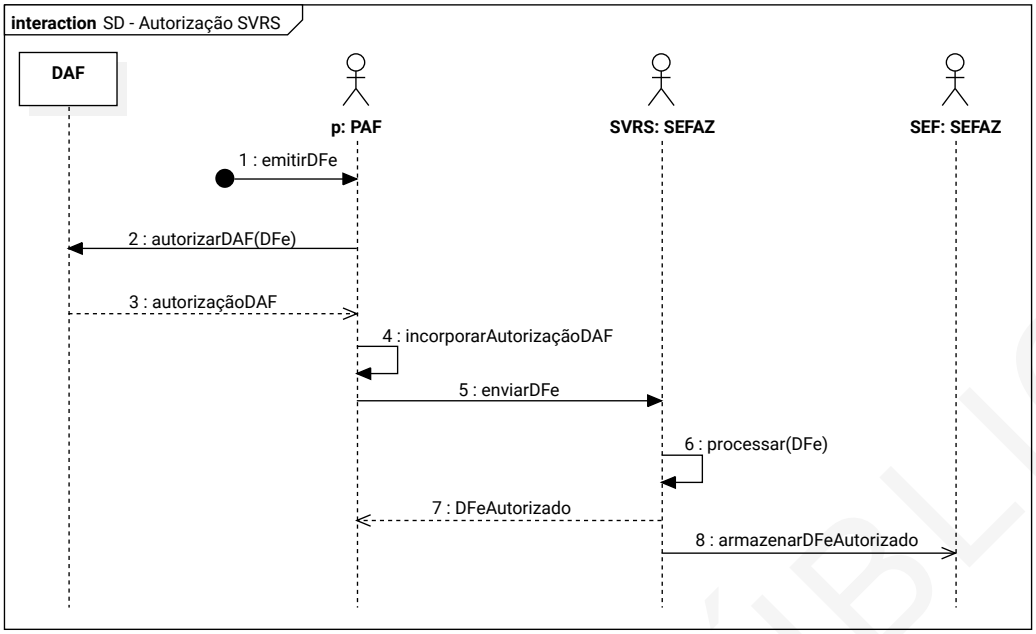
O PAF DEVE estar ciente da data de expiração do certificado digital da SEF contido em seu DAF e antes que esse expire, DEVE realizar o procedimento para substituir esse certificado.

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 Obter resultado sobre autorização de DF-e

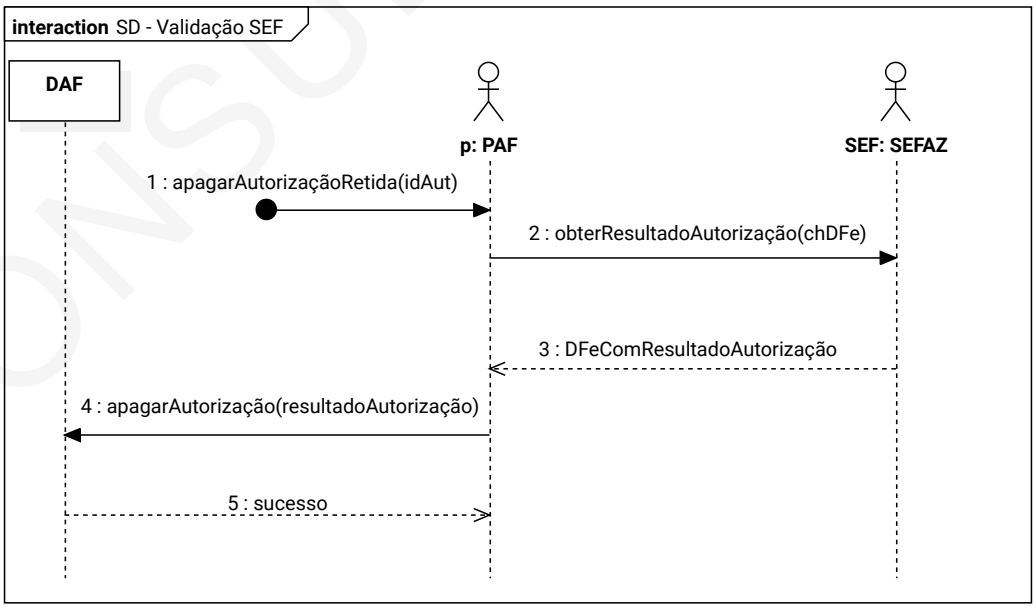
De acordo com a decisão do Grupo Especialista Setorial em Automação Comercial da SEF (GESAC), o projeto DAF será usado somente pelo estado de Santa Catarina e a validação da autorização emitida pelo DAF, incluída dentro do XML do DF-e, será validada exclusivamente pela Secretaria de Estado da Fazenda 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 e constatar que a Unidade Federada (UF) está como Santa Catarina, irá então verificar se o DF-e contém o fragmento de autorização emitido pelo DAF. Caso não contenha, será gerada uma exceção. Caso contenha, a SVRS encaminhará o DF-e à SEF para que essa faça, em um momento posterior, o validação do fragmento DAF. O contribuinte receberá da SVRS a informação que o DF-e foi autorizado (passo 8), contudo esse precisará posteriormente interagir com a SEF para que receba uma autorização que permita ao DAF excluir a autorização retida em sua MT.

Figura 7.3: Diagrama de sequência do processo de validação de autorização



Na Figura 7.3 é ilustrado um diagrama de sequência com o fluxo principal do processo de validação de uma autorização emitida pelo 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.

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.

8.1 Serviços *Web* disponibilizados

A Tabela 8.1 contém a relação de Serviços *Web*.

Tabela 8.1: Relações de Servicos *Web*

Serviço	Método	Função
DAFRegistroDispositivo	iniciarRegistro	Recepção de solicitações para iniciar registro do DAF
	confirmarRegistro	Resultado da solicitação de registro do DAF
DAFRemocaoRegistro	removerRegistro	Recepção de solicitações para remover registro do DAF
	confirmarRemoverRegistro	Resultado da remoção de registro DAF
DAFAtualizacaoCertificado	solicitarCertificado	Recepção de solicitações de atualização de certificado digital
DAFResultadoAutorizacao	obterResultadoAutorizacao	Resultado da validação da autorização do DAF
DAFConsultaSB	consultarVersaoSB	Informações sobre a versão atual do SB para um modelo de DAF
DAFConsultaDispositivo	consultarDispositivo	Consulta da situação do DAF junto à SEF
DAFAvisoExtravio	avisarExtravio	Recepção de notificação de sinistro ocorrido com o DAF
DAFSolicitarChavePAF	solicitarChavePAF	Recepção das solicitações de chave PAF

8.2 Padrões técnicos

8.2.1 Padrão de comunicação

A comunicação entre o PAF e a SEF será baseada em Serviços *Web* síncronos disponibilizados pela SEF, sendo que o envio da solicitação e a obtenção do retorno serão realizados na mesma conexão através de um único método. O meio de comunicação será a Internet, com uso do protocolo TLS com

versão igual ou superior ao utilizado no ENCAT (2019a).

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*.

1. A chamada de serviços referentes ao DAF 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;
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. 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 8.5.

Listagem 8.1: Exemplo de mensagem de requisição SOAP

```
<?xml version="1.0" encoding="utf-8"?>
<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">
 <soap12:Body>
  <iniciarRegistro xmlns="http://www.portalfiscal.inf.br/daf/wsdl/DAFRegistroDispositivo">
   <!-- Conteúdo do pedido -->
  </iniciarRegistro>
 </soap12:Body>
</soap12:Envelope>
```

Listagem 8.2: Exemplo de mensagem de retorno SOAP

```
<?xml version="1.0" encoding="utf-8"?>
<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">
 <soap12:Body>
  <iniciarRegistroResponse xmlns="http://www.portalfiscal.inf.br/daf/wsdl/DAFRegistroDispositivo">
   <!-- Conteúdo da resposta -->
  </iniciarRegistroResponse>
 </soap12:Body>
</soap12:Envelope>
```

8.2.2 Padrão de assinatura digital

1. As mensagens enviadas à SEF são documentos eletrônicos elaborados no padrão XML e devem ser assinados digitalmente com um certificado digital emitido por 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.

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

```
<iniciarRegistro xmlns="http://www.portalfiscal.inf.br/daf/wsdl/DAFRegistroDispositivo">
  <pedRegistro xmlns="http://www.portalfiscal.inf.br/daf" versao="1.00">
    <infRegistro Id="ughyrcDYBW0zaIGJG3Z6iw">
    <!-- Conteúdo do pedido -->
    </infRegistro>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <Reference URI="#ughyrcDYBW0zaIGJG3Z6iw">
          <Transforms>
            <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
          </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <DigestValue>dQXTK2bjTzPLEWKGztY8wuv7f20=</DigestValue>
        </Reference>
      </SignedInfo>
      <SignatureValue>vhqZ3zpWq58OPRyYJdGsKw7JX+oEwYW2wPRpAIgobsC...</SignatureValue>
      <KeyInfo>
        <X509Data>
          <X509Certificate>MIIDjzCCAnegAwIBAgIEF2/aITANBgkqhkiG9w...</X509Certificate>
        </X509Data>
      </KeyInfo>
    </Signature>
  </pedRegistro>
</iniciarRegistro>
```

8.3 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 a codificação dos caracteres é 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 na própria *tag* `Signature`.

Na Tabela 8.2 são apresentadas os nomes das colunas, bem como suas descrições, das tabelas com as definições de leiaute XML que são apresentadas nesse 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
		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		

8.4 Representação de tokens JWT

1. No cabeçalho (*header*) do *token* JWT (JONES; BRADLEY; SAKIMURA, 2015) vão constar somente as chaves `typ` e `alg`, com seus respectivos valores, com informacões sobre o algoritmo criptográfico utilizado para gerar a assinatura do *token*.

    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, 2015).

2. No conteúdo (*payload*) do *token* JWT os nomes dos parâmetros e seus valores são representados como pares chave e valor e estarão na mesma ordem dentro do documento JSON conforme apresentado nas seções neste capítulo que descrevem os métodos dos Serviços Web.

8.5 Regras de validação dos Serviços *Web*

8.5.1 Regras de validação gerais

Serão aplicadas, em todos os Serviços *Web*, as regras de validação gerais 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

8.5.2 Regras de negócio específicas

A Tabela 8.4 contém 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

A Tabela 8.5 contém 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: *hash* do IdPAF diverge do calculado
2003	Rejeição: algoritmo criptográfico inválido
2004	Rejeição: tamanho da chave criptográfica inválido
2005	Rejeição: *nonce* não corresponde ao informado pela SEF
2006	Rejeição: par de chave privada e chave pública do DAF não são correspondentes
2007	Rejeição: assinatura gerada pela chave de ateste não corresponde a um modelo de DAF certificado
2008	Rejeição: valor do contador monotônico inválido
2009	Rejeição: assinatura de *token* inválida
2010	Rejeição: CNPJ do responsável técnico inválido.
2011	Rejeição: identificador do CSRT (tag:idCSRT) não cadastrado na SEF
2012	Rejeição: identificador do CSRT (tag:idCSRT) revogado
2013	Rejeição: *hash* do idDAF e do contador monotônico diverge do calculado
2014	Rejeição: CNPJ do contribuinte inválido
2015	Rejeição: CNPJ do contribuinte não cadastrado
2016	Rejeição: CNPJ do responsável técnico diverge do cadastrado
2017	Rejeição: CNPJ do responsável técnico não cadastrado
2018	Rejeição: IdPAF não registrado
2019	Rejeição: DAF extraviado
2020	Rejeição: IdDAF do *token* não corresponde ao idDAF informado
2021	Rejeição: chave DF-e não foi encontrada

2022	Rejeição: idDAF do requerente não corresponde ao idDAF de autorização do DF-e
2023	Rejeição: DAF em situação irregular
2024	Rejeição: IdPAF inválido
2025	Rejeição: notificação de extravio do DAF já foi realizada
2026	Rejeição: DAF deve atualizar a versão do software básico
2027	Rejeição: versão do software básico do DAF está desatualizada

8.6 Serviço *Web* - `DAFRegistroDispositivo`

Este serviço permite ao PAF do contribuinte registrar seu DAF junto à SEF e o processo operacional está descrito na Subseção 7.6.1.

8.6.1 `iniciarRegistro`

- **Função:** serviço destinado ao atendimento de solicitações para iniciar o processo de registro de DAF.
- **Processo:** síncrono.
- **Método:** `iniciarRegistro`

8.6.1.1 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
DRP01	`pedRegistro`	Raiz	-	-	-	-	TAG raiz
DRP02	`versao`	A	DRP01	C	1-1	4	versão do leiaute
DRP03	`infRegistro`	G	DRP01	-	1-1	-	grupo de informações necessárias para o registro do DAF
DRP04	`Id`	ID	DRP03	C	1-1	22	identificador da TAG a ser assinada. Deve-se informar o idDAF representado em Base64URL
DRP05	`idDAF`	E	DRP03	C	1-1	22	Identificador único do DAF representado em Base64URL
DRP06	`algoritmosDAF`	G	DRP03	-	1-12	-	informações sobre algoritmos criptográficos
DRP07	`alg`	E	DRP06	C	1-1	5	algoritmo criptográfico que o DAF é capaz de operar
DRP08	`tamChave`	E	DRP06	N	1-1	4	tamanho da chave criptográfica que o DAF é capaz de operar
DRP09	`cnpjContribuinte`	E	DRP03	C	1-1	14	CNPJ do contribuinte
DRP10	`idPAF`	E	DRP03	C	1-1	43	Identificador único do PAF
DRP11	`cnpjResponsavel`	E	DRP03	C	1-1	14	CNPJ do responsável técnico
DRP12	`idCSRT`	E	DRP03	N	1-1	1	identificador do CSRT
DRP13	`Signature`	G	DRP01	xml	1-1	-	assinatura XML do grupo identificado pelo atributo `Id`

8.6.1.2 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
DRR01	`retRegistro`	Raiz	-	-	-	-	TAG raiz
DRR02	`versao`	A	DRR01	C	1-1	4	versão do leiaute
DRR03	`idDAF`	E	DRR01	C	1-1	22	Identificador único do DAF
DRR04	`cStat`	E	DRR01	N	1-1	3-4	código de *status* da resposta (Veja Tabela 8.9)
DRR05	`xMotivo`	E	DRR01	C	1-1	1-255	descrição literal do *status* da resposta
DRR06	`tkDesafio`	E	DRR01	C	0-1	300-500	*token* JWT contendo o desafio gerado pela SEF. (Veja Tabela 8.8)

O campo `DRR06`, indicado na Tabela 8.7, tem por objetivo conter um *token* JWT (Veja Seção 8.4), cujo conteúdo (*payload*) está descrito na Tabela 8.8.

Tabela 8.8: Conteúdo do *token* `tkDesafio`

Nome do parâmetro	Tamanho (*bytes)*	Tipo	Descrição
`nonce`	22	*string*	valor aleatório gerado pela SEF representado em Base64URL.

8.6.1.3 Validações

Serão aplicadas as validações das regras de negócio apresentadas na Tabela 8.9.

Tabela 8.9: Validação da mensagem de entrada do método `iniciarRegistro`

#	Descrição	Código	Efeito
VRP01	CNPJ do responsável técnico inválido	2010	rejeição
VRP02	CNPJ do responsável técnico não cadastrado	2017	rejeição
VRP03	CNPJ do responsável técnico diverge do cadastrado	2016	rejeição
VRP04	CNPJ do contribuinte inválido	2014	rejeição
VRP05	CNPJ do contribuinte não cadastrado	2015	rejeição
VRP06	identificador do CSRT (tag:idCSRT) não cadastrado na SEF	2011	rejeição
VRP07	identificador do CSRT (tag:idCSRT) revogado	2012	rejeição
VRP08	algoritmo de chave criptográfica inválido	2003	rejeição
VRP09	tamanho da chave criptográfica inválido	2004	rejeição
VRP10	IdPAF inválido	2024	rejeição

8.6.1.4 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.

8.6.2 `confirmarRegistro`

- **Função:** serviço destinado a efetivar o registro do DAF junto à SEF.
- **Processo:** síncrono.
- **Método:** `confirmarRegistro`

8.6.2.1 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
DRE01	`pedConfRegistro`	Raiz	-	-	-	-	TAG raiz
DRE02	`versao`	A	DRE01	C	1-1	4	versão do leiaute
DRE03	`infConfRegistro`	G	DRE01	-	1-1	-	informações para a confirmação do registro
DRE04	`Id`	ID	DRE03	C	1-1	22	identificador da TAG a ser assinada. Deve-se informar o idDAF representado em Base64URL
DRE05	`tkAut`	E	DRE03	C	1-1	2.900-3.100	*token* JWT com informações para registro (Veja Tabela 8.11).
DRE06	`idDAF`	E	DRE03	C	1-1	22	Identificador único do DAF representado em Base64URL
DRE07	`idPAF`	E	DRE03	C	1-1	43	Identificador único do PAF
DRE08	`Signature`	G	DRE01	xml	1-1	-	assinatura XML do grupo identificado pelo atributo `Id`

O campo `DRE05`, indicado na Tabela 8.10, tem por objetivo conter um *token* JWT (Veja Seção 8.4) 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 informacões apresentadas na Tabela 8.11.

Tabela 8.11: Conteúdo do *token* JWT que está associado à chave jwt contida no campo tkAut

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
`idDAF`	22	*string*	IdDAF representado em Base64URL
`cont`	4	inteiro	valor atual do contador monotônico
`nonce`	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 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
DCR01	`retConfRegistro`	Raiz	-	-	-	-	TAG raiz
DCR02	`versao`	A	DCR01	C	1-1	4	versão do leiaute
DCR03	`idDAF`	E	DCR01	C	1-1	22	Identificador único do DAF
DCR04	`cStat`	E	DCR01	N	1-1	3-4	código de *status* da resposta (Veja Tabela 8.14)
DCR05	`xMotivo`	E	DCR01	C	1-1	1-255	descrição literal do status da resposta
DCR06	`tkChaves`	E	DCR01	C	0-1	850-1.050	JWT contendo as informações de retorno do registro. (Veja Tabela 8.13)

O campo `DCR06`, indicado na Tabela 8.12, tem por objetivo conter um *token* JWT (Veja Seção 8.4), cujo conteúdo (*payload*) está descrito na Tabela 8.13.

Tabela 8.13: Conteúdo do *token* `tkChaves`

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
`chSEF`	variável	*string*	Chave SEF cifrada com a chave pública do DAF, com o esquema de cifragem `RSAES-OAEP` (MORIARTY et al., 2016), e representada em Base64URL
`chPAF`	86	*string*	Chave PAF representada em Base64URL

8.6.2.3 Validações

Serão aplicadas as validações das regras de negócio apresentadas na Tabela 8.14.

Tabela 8.14: Validação da mensagem de entrada do método `confirmarRegistro`

#	Descrição	Código	Efeito
VRC01	IdDAF do *token* não corresponde ao idDAF informado	2020	rejeição
VRC02	*nonce* não corresponde ao informado pela SEF	2005	rejeição
VRC03	par de chave privada e chave pública do DAF não são correspondentes	2006	rejeição
VRC04	assinatura gerada pela chave de ateste não corresponde a uma modelo de DAF certificado pela SEF	2007	rejeição
VRC05	IdPAF inválido	2024	rejeição

8.6.2.4 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.

8.7 Serviço *Web* - DAFRemocaoRegistro

Serviço destinado a remover as informações de registro do DAF junto à SEF. O processo operacional está descrito na Subseção 7.6.2.

8.7.1 removerRegistro

- **Função:** serviço destinado a solicitar a remoção das informações de registro do DAF junto à SEF.
- **Processo:** síncrono.
- **Método:** removerRegistro

8.7.1.1 Leiaute mensagem de entrada

Entrada: estrutura XML da mensagem para a solicitação de 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
PRD01	pedRemRegistro	Raiz	-	-	-	-	TAG raiz
PRD02	versao	A	PRD01	C	1-1	4	versão do leiaute
PRD03	infRemRegistro	G	PRD01	-	1-1	-	informações para a solicitação de remoção do registro
PRD04	Id	ID	PRD03	C	1-1	22	identificador da TAG a ser assinada. Deve-se informar o idDAF representado em Base64URL
PRD05	idDAF	E	PRD03	C	1-1	22	Identificador único do DAF representado em Base64URL
PRD06	idPAF	E	PRD03	C	1-1	43	Identificador único do PAF
PRD07	xJust	E	PRD03	C	1-1	15-255	justificativa da remoção de registro
PRD08	Signature	G	PRD01	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 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
RRD01	retRemRegistro	Raiz	-	-	-	-	TAG raiz
RRD02	versao	A	RRD01	C	1-1	4	versão do leiaute
RRD03	idDAF	E	RRD01	C	1-1	22	Identificador único do DAF representado em Base64URL
RRD04	cStat	E	RRD01	N	1-1	3-4	código de *status* da resposta (Veja Tabela 8.18)

RRD05	xMotivo	E	RRD01	C	1-1	1-255	descrição literal do *status* da resposta
RRD06	tkDesafio	E	RRD01	C	0-1	300-500	*token* JWT (Veja Tabela 8.16)

O campo RRD06, indicado na Tabela 8.16, tem por objetivo conter um *token* JWT (Veja Seção 8.4), cujo conteúdo (*payload*) está descrito na Tabela 8.17.

Tabela 8.17: Conteúdo do *token* tkDesafio

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
nonce	22	*string*	valor aleatório gerado pela SEF representado em Base64URL

8.7.1.3 Validações

Serão aplicadas as validações das regras de negócio apresentadas na Tabela 8.18.

Tabela 8.18: Validação da mensagem de entrada do método removerRegistro

#	Descrição	Código	Efeito
VRD01	registro do IdDAF não encontrado	2000	rejeição
VRD02	IdPAF não corresponde ao registro do DAF	2001	rejeição
VRD03	DAF extraviado	2019	rejeição
VRD04	DAF em situação irregular	2023	rejeição

8.7.1.4 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.

8.7.2 confirmarRemoverRegistro

- **Função:** serviço destinado a confirmar a remoção das informações de registro do DAF junto à SEF.
- **Processo:** síncrono.
- **Método:** confirmarRemoverRegistro

8.7.2.1 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 confirmarRemoverRegistro

#	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	22	identificador da TAG a ser assinada. Deve-se informar o idDAF representado em Base64URL
PCR05	tkAut	E	PCR03	C	1-1	400-600	*token* JWT (Veja Tabela 8.20)
PCR06	idDAF	E	PCR03	C	1-1	22	Identificador único do DAF representado em Base64URL
PCR07	idPAF	E	PCR03	C	1-1	43	Identificador único do PAF
PCR08	Signature	G	PCR01	xml	1-1	-	assinatura XML do grupo identificado pelo atributo Id

O campo PCR05, indicado na Tabela 8.19, tem por objetivo conter um *token* JWT (Veja Seção 8.4), cujo conteúdo (*payload*) está descrito na Tabela 8.20.

Tabela 8.20: Conteúdo do *token* tkAut

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
idDAF	22	*string*	Identificador único do DAF representado em Base64URL
cont	4	inteiro	valor atual do contador monotônico
nonce	22	*string*	valor aleatório gerado pela SEF representado em Base64URL

8.7.2.2 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 confirmarRemoverRegistro

#	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 *status* da resposta (Veja Tabela 8.23)
RCR05	xMotivo	E	RCR01	C	1-1	1-255	descrição literal do *status* 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 8.4), cujo conteúdo (*payload*) está descrito na Tabela 8.22.

Tabela 8.22: Conteúdo do *token* tkEvento

Nome do parâmetro	Tamanho (*bytes*)	Tipo	Descrição
evento	7	*string*	cadeia de caracateres REMOVER

8.7.2.3 Validações

Serão aplicadas as validações das regras de negócio apresentadas na Tabela 8.23.

Tabela 8.23: Validação da mensagem de entrada do método `confirmarRemoverRegistro`

#	Descrição	Código	Efeito
VCR01	registro do IdDAF não encontrado	2000	rejeição
VCR02	IdPAF não corresponde ao registro do DAF	2001	rejeição
VCR03	valor do contador monotônico inválido	2008	rejeição
VCR04	par de chave privada e chave pública do DAF não são correspondentes	2006	rejeição
VCR05	IdDAF do *token* não corresponde ao idDAF informado	2020	rejeição
VCR06	*nonce* não corresponde ao informado pela SEF	2005	rejeição

8.7.2.4 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.

8.8 Serviço *Web* - `DAFConsultaSB`

Este serviço permite ao PAF do contribuinte consultar a versão atual do *Software* Básico disponibilizada pela SEF. O processo operacional está descrito na Subseção 7.6.3.

8.8.1 `consultarVersaoSB`

- **Função:** serviço destinado à consulta de informações sobre a versão atual do SB disponibilizado pela SEF.
- **Processo:** síncrono.
- **Método:** `consultarVersaoSB`

8.8.1.1 Leiaute mensagem de entrada

Entrada: estrutura XML da mensagem de entrada para consulta da versão do SB (Veja Tabela 8.24).

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

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PCS01	`pedConsVersaoSB`	Raiz	-	-	-	-	TAG raiz
PCS02	`versao`	A	PCS01	C	1-1	4	versão do leiaute
PCS03	`infConsVersaoSB`	G	PCS01	-	1-1	-	informações para o consulta do SB
PCS04	`Id`	ID	PCS03	C	1-1	22	identificador da TAG a ser assinada. Deve-se informar o idDAF representado em Base64URL
PCS05	`idDAF`	E	PCS03	C	1-1	22	Identificador único do DAF representado em Base64URL

PCS06	idPAF	E	PCS03	C	1-1	43	Identificador único do PAF
PCS07	Signature	G	PCS01	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 consulta da versão do SB (Veja Tabela 8.25).

Tabela 8.25: 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	dataSB	E	RCS01	D	1-1	-	data do lançamento da versão no formato "AAAA-MM-DD"
RCS05	versaoSB	E	RCS01	C	1-1	8	versão do SB
RCS06	urlSB	E	RCS01	C	1-1	15-2.000	URL onde o SB está disponível
RCS07	resumoCripSB	E	RCS01	C	1-1	43	resumo criptográfico do SB, representado em Base64URL
RCS08	cStat	E	RCS01	N	1-1	3-4	código *status* da resposta (Veja Tabela 8.26)
RCS09	xMotivo	E	RCS01	C	1-1	1-255	descrição literal do *status* da resposta

8.8.1.3 Validações

Serão aplicadas as validações das regras de negócio apresentadas na Tabela 8.26.

Tabela 8.26: Validação da mensagem de entrada do método consultarVersaoSB

#	Descrição	Código	Efeito
VCS01	IdPAF não registrado	2018	rejeição

8.8.1.4 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 8.26.

8.9 Serviço *Web* - DAFAtualizacaoCertificado

Este serviço é responsável por realizar a atualização do certificado digital da SEF do DAF junto à SEF. O processo operacional está descrito na Subseção 7.6.7.

8.9.1 solicitarCertificado

- **Função:** serviço destinado a solicitar a atualização do certificado digital da SEF.

- **Processo:** síncrono.
- **Método:** `solicitarCertificado`

8.9.1.1 Leiaute mensagem de entrada

Entrada: estrutura XML da mensagem de entrada da solicitação de atualização do certificado digital da SEF (Veja Tabela 8.27).

Tabela 8.27: 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	22	identificador da TAG a ser assinada. Deve-se informar o idDAF representado em Base64URL
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	`Signature`	G	PSC01	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 da solicitação de atualização do certificado digital da SEF (Veja Tabela 8.28).

Tabela 8.28: 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	`certificado`	E	RCS01	C	1-1	1-2.000	novo certificado digital da SEF codificado no formato textual (Veja (JOSEFSSON; LEONARD, 2015))
RSC05	`idDAF`	E	RSC01	C	1-1	22	Identificador único do DAF
RSC04	`cStat`	E	RSC01	N	1-1	3-4	código de *status* da resposta (Veja Tabela 8.29)
RSC06	`xMotivo`	E	RSC01	C	1-1	1-255	descrição literal do *status* da resposta

8.9.1.3 Validações

Serão aplicadas as validações das regras de negócio apresentadas na Tabela 8.29.

Tabela 8.29: Validação da mensagem de entrada do método `solicitarCertificado`

#	Descrição	Código	Efeito
VSC01	IdPAF não registrado	2018	rejeição

8.9.1.4 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 8.29.

8.10 Serviço *Web* - `DAFResultadoAutorizacao`

Serviço destinado a obter o resultado da validação do fragmento DAF junto à SEF. O processo operacional está descrito na Subseção 7.6.8.

8.10.1 `obterResultadoAutorizacao`

- **Função:** serviço destinado a obter o resultado da validação do fragmento DAF.
- **Processo:** assíncrono.
- **Método:** `obterResultadoAutorizacao`

8.10.1.1 Leiaute mensagem de entrada

Entrada: estrutura XML da mensagem para a solicitação do resultado do processamento do fragmento DAF (Veja Tabela 8.30).

Tabela 8.30: Leiaute da mensagem de entrada do método `obterResultadoAutorizacao`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PRA01	`pedAutorizacao`	Raiz	-	-	-	-	TAG raiz
PRA02	`versao`	A	PRA01	C	1-1	4	versão do leiaute
PRA03	`infAutorizacao`	G	PRA01	-	1-1	-	informações para o processamento do fragmento DAF
PRA04	`Id`	ID	PRA03	C	1-1	22	identificador da TAG a ser assinada. Deve-se informar o idDAF representado em Base64URL
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`

8.10.1.2 Leiaute mensagem de retorno

Retorno: estrutura XML da mensagem de retorno do resultado do processamento do fragmento DAF (Veja Tabela 8.31).

Tabela 8.31: 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 *status* da resposta (Veja Tabela 8.33)
RRA05	`xMotivo`	E	RRA01	C	1-1	1-255	descrição literal do *status* 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 *status* da resposta de autorização (Veja Tabela 8.32)
RRA11	`xMotAut`	E	RRA06	C	1-1	1-255	descrição literal do *status* da resposta de autorização

8.10.1.3 Validações

Serão aplicadas as regras de validação do resultado do processamento do fragmento DAF da Tabela 8.32 para cada chave de acesso de DF-e.

Tabela 8.32: Validação do processamento do fragmento DAF

#	Descrição	Código	Efeito
VCA01	chave DF-e não foi encontrada	2021	rejeição
VCA02	idDAF do requerente não corresponde ao idDAF de autorização do DF-e	2022	rejeição

Além disso serão aplicadas as regras de validação das regras de negócio da Tabela 8.33.

Tabela 8.33: Validação da mensagem de entrada do método `obterResultadoAutorizacao`

#	Descrição	Código	Efeito
VRA01	DAF em situação irregular	2023	rejeição
VRA02	IdPAF não corresponde ao registro do DAF	2001	rejeição
VRA03	valor do contador monotônico inválido	2008	rejeição
VRA04	DAF extraviado	2019	rejeição

VRA05	DAF deve atualizar a versão do software básico	2026	rejeição
VRA06	versão do software básico do DAF está desatualizada	2027	rejeição

8.10.1.4 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 8.32 e a Tabela 8.33.

8.11 Serviço *Web* - `DAFConsultaDispositivo`

Serviço destinado a consultar a situação do DAF junto à SEF. O processo operacional está descrito na Subseção 7.6.4.

8.11.1 `consultarDispositivo`

- **Função:** serviço destinado a consultar a situação do DAF junto à SEF.
- **Processo:** síncrono.
- **Método:** `consultarDispositivo`

8.11.1.1 Leiaute mensagem de entrada

Entrada: estrutura XML da mensagem de entrada de consulta do DAF (Veja Tabela 8.34).

Tabela 8.34: Leiaute da mensagem de entrada do método `consultarDispositivo`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PSD01	`pedSituacao`	Raiz	-	-	-	-	TAG raiz
PSD02	`versao`	A	PSD01	C	1-1	4	versão do leiaute
PSD03	`infSituacao`	G	PSD01	-	1-1	-	informações para a consulta do DAF
PSD04	`Id`	ID	PSD03	C	1-1	22	identificador da TAG a ser assinada. Deve-se informar o idDAF representado em Base64URL
PSD05	`idDAF`	E	PSD03	C	1-1	22	Identificador único do DAF representado em Base64URL
PSD06	`idPAF`	E	PSD03	C	1-1	43	Identificador único do PAF
PSD07	`Signature`	G	PSD01	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 de consulta do DAF (Veja Tabela 8.35).

Tabela 8.35: Leiaute da mensagem de retorno do método `consultarDispositivo`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
RSD01	`retConsultaDAF`	Raiz	-	-	-	-	TAG raiz

RSD02	versao	A	RSD01	C	1-1	4	versão do leiaute
RSD03	idDAF	E	RSD01	C	1-1	36	Identificador único do DAF
RSD04	idPAF	E	RSD03	C	1-1	43	Identificador único do PAF
RSD05	ultimaVersaoSB	E	RSD01	C	1-1	8	última versão disponível de SB
RSD06	dataRegistro	E	RSD01	D	0-1	-	Data de registro - Formato: "AAAA-MM-DD"
RSD07	algoritmosDAF	G	RSD01	-	1-12	-	informações sobre algoritmos criptográficos
RSD08	alg	E	RSD07	C	1-1	5	algoritmo criptográfico que o DAF é capaz de operar
RSD09	tamChave	E	RSD07	N	1-1	4	tamanho da chave criptográfica que o DAF é capaz de operar
RSD10	cnpjContribuinte	E	RSD01	C	0-1	14	CNPJ do contribuinte
RSD11	cnpjResponsavel	E	RSD01	C	0-1	14	CNPJ do responsável técnico
RSD12	idCSRT	E	RSD01	N	0-1	1	identificador do CSRT
RSD13	xSituacao	E	RSD01	C	0-1	1-255	descrição da situação do DAF junto à SEF (por exemplo: REGULAR, INATIVO, EXTRAVIADO)
RSD14	cStat	E	RSD01	N	1-1	3-4	código de *status* da resposta (Veja Tabela 8.36)
RSD15	xMotivo	E	RSD01	C	1-1	1-255	descrição literal do *status* da resposta

8.11.1.3 Validações

Serão aplicadas as validações das regras de negócio apresentadas na Tabela 8.36.

Tabela 8.36: Validação da mensagem de entrada do método `consultarDispositivo`

#	Descrição	Código	Efeito
VSD01	registro do IdDAF não encontrado	2000	rejeição
VSD02	IdPAF não corresponde ao registro do DAF	2001	rejeição

8.11.1.4 Final do processamento

Em caso de sucesso o processamento da consulta da situação do DAF retorna as informações referente ao dispositivo e o `cStat` com o valor 1000 da Tabela 8.4. Caso contrário, resulta em uma mensagem de erro conforme Tabela 8.36.

8.12 Serviço *Web* - `DAFAvisoExtravio`

Serviço destinado a notificar à SEF de sinistro ocorrido com o DAF. O processo operacional está descrito na Subseção 7.6.6.

8.12.1 `avisarExtravio`

- **Função:** serviço destinado a notificar à SEF de sinistro ocorrido com o DAF.
- **Processo:** síncrono.

- **Método:** `avisarExtravio`

8.12.1.1 Leiaute mensagem de entrada

Entrada: estrutura XML da mensagem de entrada de notificação de extravio do DAF (Veja Tabela 8.37).

Tabela 8.37: Leiaute da mensagem de entrada do método `avisarExtravio`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PNE01	`pedExtravio`	Raiz	-	-	-	-	TAG raiz
PNE02	`versao`	A	PNE01	C	1-1	4	versão do leiaute
PNE03	`infExtravio`	G	PNE01	-	1-1	-	informações da notificação de extravio do DAF
PNE04	`Id`	ID	PNE03	C	1-1	22	identificador da TAG a ser assinada. Deve-se informar o idDAF representado em Base64URL
PNE05	`idDAF`	E	PNE03	C	1-1	22	Identificador único do DAF representado em Base64URL
PNE06	`idPAF`	E	PNE03	C	1-1	43	Identificador único do PAF
PNE07	`xJust`	E	PNE03	C	1-1	15-256	descrição do sinistro ocorrido com o DAF
PNE08	`Signature`	G	PNE01	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 de notificação de extravio do DAF (Veja Tabela 8.38).

Tabela 8.38: Leiaute da mensagem de retorno do método `avisarExtravio`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
RNE01	`retExtravio`	Raiz	-	-	-	-	TAG raiz
RNE02	`versao`	A	RNE01	C	1-1	4	versão do leiaute
RNE03	`idDAF`	E	RNE01	C	1-1	22	Identificador único do DAF
RNE04	`cStat`	E	RNE01	N	1-1	3-4	código de *status* da resposta (Veja Tabela 8.39)
RNE05	`xMotivo`	E	RNE01	C	1-1	1-255	descrição literal do *status* da resposta

8.12.1.3 Validações

Serão aplicadas as validações das regras de negócio apresentadas na Tabela 8.39.

Tabela 8.39: Validação da mensagem de entrada do método `avisarExtravio`

#	Descrição	Código	Efeito
VNE01	registro do IdDAF não encontrado	2000	rejeição

VNE02	IdPAF não corresponde ao registro do DAF	2001	rejeição
VNE03	notificação de extravio do DAF já foi realizada	2025	rejeição

8.12.1.4 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 8.39.

8.13 Serviço *Web* - `DAFSolicitarChavePAF`

Serviço destinado à recuperação pelo PAF da chave PAF junto à SEF. O processo operacional está descrito na Subseção 7.6.5.

8.13.1 `solicitarChavePAF`

- **Função:** serviço destinado à solicitação de uma nova chave PAF junto à SEF.
- **Processo:** síncrono.
- **Método:** `solicitarChavePAF`

8.13.1.1 Leiaute mensagem de entrada

Entrada: estrutura XML da mensagem de entrada de solicitação de chave PAF (Veja Tabela 8.40).

Tabela 8.40: Leiaute da mensagem de entrada do método `solicitarChavePAF`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
PNC01	`pedChavePAF`	Raiz	-	-	-	-	TAG raiz
PNC02	`versao`	A	PNC01	C	1-1	4	versão do leiaute
PNC03	`infChavePAF`	G	PNC01	-	1-1	-	informações para solicitação da chave PAF
PNC04	`Id`	ID	PNC03	C	1-1	22	identificador da TAG a ser assinada. Deve-se informar o idDAF representado em Base64URL
PNC05	`idDAF`	E	PNC03	C	1-1	22	Identificador único do DAF representado em Base64URL
PNC06	`idPAF`	E	PNC03	C	1-1	43	Identificador único do PAF
PNC07	`Signature`	G	PNC01	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 solicitação de chave PAF (Veja Tabela 8.41).

Tabela 8.41: Leiaute da mensagem de retorno do método `solicitarChavePAF`

#	Campo	Elemento	Pai	Tipo	Ocorr.	Tamanho	Descrição
RNC01	`retChavePAF`	Raiz	-	-	-	-	TAG raiz

RNC02	`versao`	A	RNC01	C	1-1	4	versão do leiaute
RNC03	`idPAF`	E	RNC01	C	1-1	43	Identificador único do PAF
RNC04	`chavePAF`	E	RNC01	C	1-1	86	chave PAF representada em Base64URL
RNC05	`cStat`	E	RNC01	N	1-1	3-4	código de *status* da resposta (Veja Tabela 8.42)
RNC06	`xMotivo`	E	RNC01	C	1-1	1-255	descrição literal do *status* da resposta

8.13.1.3 Validações

Serão aplicadas as validações das regras de negócio apresentadas na Tabela 8.42.

Tabela 8.42: Regras de validação da mensagem de entrada do método `solicitarChavePAF`

#	Descrição	Código	Efeito
VNC01	IdPAF não registrado	2018	rejeição

8.13.1.4 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 8.42.

Referências

BRADNER, Scott. *Key words for use in RFCs to Indicate Requirement Levels*. Mar. 1997. Disponível em: <http://www.rfc-editor.org/rfc/rfc2119.txt>.

BRAY, T. *The JavaScript Object Notation (JSON) Data Interchange Format*. Dez. 2017. Disponível em: <https://www.rfc-editor.org/rfc/rfc8259.html>.

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: <http://www.rfc-editor.org/rfc/rfc5280.txt>.

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: <http://www.rfc-editor.org/rfc/rfc7518.txt>.

_____. *JSON Web Key (JWK)*. Mai. 2015. Disponível em: <http://www.rfc-editor.org/rfc/rfc7517.txt>.

JONES, M.; BRADLEY, J.; SAKIMURA, N. *JSON Web Token (JWT)*. Mai. 2015. Disponível em: <http://www.rfc-editor.org/rfc/rfc7519.txt>.

JOSEFSSON, S. *The Base16, Base32, and Base64 Data Encodings*. Out. 2006. Disponível em: <http://www.rfc-editor.org/rfc/rfc4648.txt>.

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: <http://www.rfc-editor.org/rfc/rfc2104.txt>.

LEACH, Paul J.; MEALLING, Michael; SALZ, Rich. *A Universally Unique IDentifier (UUID) URN Namespace*. Jul. 2005. Disponível em: <http://www.rfc-editor.org/rfc/rfc4122.txt>.

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

NIST. *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: <http://www.rfc-editor.org/rfc/rfc2986.txt>.

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

A Exemplos de como representar documentos JSON das mensagens da API do DAF

Os exemplos com documentos JSON apresentados nesse apêndice possuem quebras de linha e espaços em branco somente para facilitar a leitura dos mesmos. Para a comunicação entre PAF e DAF, os documentos JSON DEVEM ser gerado de acordo com a Seção 6.1.

A.1 Pedidos sem assinatura digital

A Listagem A.1 apresenta a representação de um pedido para o DAF que não contém assinatura digital e não contém parâmetros adicionais. No pedido DEVE conter apenas a chave `cmd` com o valor de acordo com a Tabela 6.1.

Listagem A.1: Documento JSON para pedidos sem assinatura digital e sem parâmetros adicionais

```
{
  "msg": 3
}
```

A Listagem A.2 apresenta a representação de um pedido para o DAF que não contém assinatura digital e contém parâmetros adicionais. No pedido DEVE conter a chave `cmd` com o valor de acordo com a Tabela 6.1, seguido dos parâmetros na sequência em que eles aparecem nas suas respectivas tabelas na Seção 6.2.

Listagem A.2: Documento JSON para pedidos sem assinatura digital e com parâmetros adicionais

```
{
  "msg": 4,
  "fragDFE": "PGluZk5GZSBJZD0iTkZlNDIyMDA4NjE1ODU4NjYwMDAxMDQ2NTAwMDgwMjQ1MjI3MTExMzA5MDAwNTQi
    IHZlcnNhbz0iNC4wMCI-PGlkZT48Y1VGPjQyPC9jVUY-PGNORj4xMzA5MDAwNTwvYO5GPjxuYXRPcD5WRU5EQSBERSBN
    RVJDQURPUklBIENPTkZPUk1FIENGT1A8L25hdE9wPjxtb2Q-NjU8L21vZD48c2VyaWU-MDwvc2VyaWU-PG5ORj44MDI0
    NTIyNzE8L25ORj48ZGhFbWk-MjAyMC0wOC0xOVQxMzozODowNC0wMzowMDwvZGhFbWk-PHRwTkY-MTwvdHBORj48aWRE
    ZXN0PjE8L2lkRGVzdD48YO11bkZHPjQyMDU0MDc8L2NNdW5GRz48dHBJbXA-NTwvdHBJbXA-PHRwRW1pcz4xPC90cEVt
    aXM-PGNEVj4OPC9jRFY-PHRwQW1iPjE8L3RwQW1iPjxmaW5ORmU-MTwvZmluTkZlPjxpbmRGaW5hbD4xPC9pbmRGaW5h
    bD48aW5kUHJlcz4xPC9pbmRQcmVzPjxwcm9jRW1pPjA8L3Byb2NFbWk-PHZlclByb2M-TkZDLWUgMS4wLjQxLjAwQ2U8
    L3ZlclByb2M-PC9pZGU-PHRvdGFsPjxJQO1TVG9OPjx2QkM-MC4wMDwvdkJDPjx2SUNNUz4wLjAwPC92SUNNUz48dklD
    TVNEZXNvbj4wLjAwPC92SUNNUORlc29uPjx2RkNQPjAuMDA8L3ZGQ1A-PHZCQ1NUPjAuMDA8L3ZCQ1NUPjx2U1Q-MC4w
```

```
    MDwvdlNUPjx2RkNQU1Q-MC4wMDwvdkZDUFNUPjx2RkNQU1RSZXQ-MC4wMDwvdkZDUFNUUmV0Pjx2UHJvZD4yMjkuOTA8
    L3ZQcm9kPjx2RnJldGU-MC4wMDwvdkZyZXRlPjx2U2VnPjAuMDA8L3ZTZWc-PHZEZXNjPjAuMDA8L3ZEZXNjPjx2SUk-
    MC4wMDwvdklJPjx2SVBJPjAuMDA8L3ZJUEk-PHZJUElEZXZvbD4wLjAwPC92SVBJRGV2b2w-PHZQSVM-MC4wMDwvdlBJ
    Uz48dkNPRklOUz4wLjAwPC92QO9GSU5TPjx2T3V0cm8-MC4wMDwvdk91dHJvPjx2TkY-MjI5LjkwPC92TkY-PHZUb3RU
    cmliPjg3LjY0PC92VG90VHJpYj48L0lDTVNUb3Q-PC90b3RhbD48L2luZk5GZT4",
  "hashDFE": "fwUV7diyXoDqM-vqShFKYWxtaWjeoGc1ZGD7L8OmHoA",
  "respDes": "mgz4EkN3hfCdqW0_Iwchc5wW5kN2z0JJHKypazbopBM"
}
```


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 resposta sem assinatura digital e sem parâmetros

```
{
    "res": 0
}
```

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 Seção 6.2.

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


```
{
  "res": 0,
  "idDAF": "ughyrcDYBW0zaIGJG3Z6iw",
  "versaoSB": "1.1.2",
  "hashSB": "CV2lZgWH662O6NuY1COMBt0YX3RrelYejwfFBaRtzUM",
  "modelo": "ughyrcDYBW0zaIGJG3Z6iw",
  "cont": 0,
  "cert": "-----BEGIN CERTIFICATE-----\nMIIDZDCCAkwCCQCZptuvvylwxDANBgkqhkiG9w0BAQsFADB0MQswCQ
    YDVQQGEwJC\nUjEXMBUGA1UECAwOU2FudGEgQ2F0YXJpbmExFjAUBgNVBAcMDUZsb3JpYW5vcG9s\naXMxDDAKBgNVBA
    oMA1NFRjEOMAwGA1UECwwFR0VTQUMxFjAUBgNVBAMMDXNlZi5z\nYy5nb3YuYnIwHhcNMjAwOTIzMTYyMDE3WhcNMzAw
    OTIxMTYyMDE3WjB0MQswCQYD\nVQQGEwJCUjEXMBUGA1UECAwOU2FudGEgQ2F0YXJpbmExFjAUBgNVBAcMDUZsb3Jp\n
    YW5vcG9saXMxDDAKBgNVBAoMA1NFRjEOMAwGA1UECwwFR0VTQUMxFjAUBgNVBAMM\nDXNlZi5zYy5nb3YuYnIwggEiM
    A0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDa\nyMjTZDIi7+JcN9t9gD8mHUDaP0byrp0rhQ9po8SkoGVkCOe1ls
    xmXi5wlY1ZNcV+\nOx+ESTcSCT4DIsNooLwhHNVmi6E93yPySJWf7aoQ57+go6dd1UA9k5Y1H2GznFAX\n77fJ2Ip4Rx
    Gz6UerRaW4luO+4gv2R9Ajxfmm/a08BqBrIznj0PJrWhJzllYe7WeS\newDjvek32PDMmeUOKAp4rD7VHW1sOSnyjBqc
    H4ipdAhZCiYM2rX1jGdFChQ39Vyg\nnOrnjVmIgAvgJKRJg12yJfDxDF77K2DHSyipygW9Ihx8xamebW4sxBvaAYR8+
    ipQ\n1dUT9T//omOMfAwV0Ex/AgMBAAEwDQYJKoZIhvcNAQELBQADggEBAMilMrIIMv3d\nwLzNqmsk7/9tk2g5pynYY
    DOtspw83JMwWOsfC8Qaucm+HKIEdP0fGWGomYLFXyYO\nBwZWK1NewcDvrGoQCyxd2NO/lhybwC3q5W3NRzS2seV/OYx
    wczHTrnrCjr1Tmd33\n/AhEqn5dXeKQnq0G1F17mJW4lRlT2FlmlvYmCSyuBUQUtkN8p/mVjsSw0KFgpG4z\nQgGlHaN
    kyje0ThuGA2tW7cxsnWF8I2H/Gt4jB+jsZcDGs5X/oYdFAv5815XVd1Kk\nWSEBltIsc3hhzEan7FEYWRsZQSRi94K7j
    LOPr7EvNjhl9i4k+8IaQXIxuI1oWD54\nLRqC7wlRu3s=\n-----END CERTIFICATE-----",
  "estado": "PRONTO",
  "retidos": ["ok9vTFrhUPYob_x8QzL6I8roxxy7mgQMCXc-0mJEesA","
    SQG9TKLAotGIfDhNFBRn2MKHbj88UdFB71bx3BhkDSo"],
  "algos": [
```

```
    {
      "alg": "RS256",
      "len": "2048"
    }
  ]
}
```

A.3 Pedidos com assinatura digital

A Listagem A.5 apresenta a representação de um pedido para o DAF que contém uma assinatura digital. No 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

```
{
  "msg": 1,
  "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJub25jZSI6Im43TlNlVDNCLWxJZklUbWFPaDdSY3cifQ.
    Ds8lHO1j-u_1IJecMxzl_2TZ4Xc9aA1lfgZa7yAFZpjtNoObkoSbZqb8B3qwcJrAXq97SJIJLsnKP36q2TjDDhPpDo
    zoVq2EndO_Qn9IFbZFPszaaXUx04ze86LXyXln8R-B0f2y3n4ueyMs9lGwf-ihiRgcHSvz3nTtv39-F-M9bHhQ8I9l
    LtUtz47XXzEhjIZPZwj0iHOxgRJdkSNtO7pVbJP6_nY0UTekcYGxlEATkPxmTH4AEcjQ5x8eq5PUDCpXCzXE6wX_cy
    hNp-3uIhghoF9-5RHMerIg4526_nGrMiPDABFvOGiX-xgIO-m43UUyhRKRec3nV624pZhVMg"
}
```

A.4 Respostas com assinatura digital

A Listagem A.6 apresenta a representação de uma resposta do DAF que contém uma assinatura digital. No 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

```
{
  "res": 0,
  "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJub25jZSI6Im43TlNlVDNCLWxJZklUbWFPaDdSY3cifQ.
    Ds8lHO1j-u_1IJecMxzl_2TZ4Xc9aA1lfgZa7yAFZpjtNoObkoSbZqb8B3qwcJrAXq97SJIJLsnKP36q2TjDDhPpDo
    zoVq2EndO_Qn9IFbZFPszaaXUx04ze86LXyXln8R-B0f2y3n4ueyMs9lGwf-ihiRgcHSvz3nTtv39-F-M9bHhQ8I9l
    LtUtz47XXzEhjIZPZwj0iHOxgRJdkSNtO7pVbJP6_nY0UTekcYGxlEATkPxmTH4AEcjQ5x8eq5PUDCpXCzXE6wX_cy
    hNp-3uIhghoF9-5RHMerIg4526_nGrMiPDABFvOGiX-xgIO-m43UUyhRKRec3nV624pZhVMg"
}
```

B Exemplos de mensagens por processos operacionais com o DAF

Neste capítulo são apresentados exemplos de mensagens do DAF e serviços providos pela SEF. Organizados por processos operacionais, 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-4.6.

B.1.1 Mensagem DAF `consultarInformacoes`

B.1.1.1 Pedido - mensagem 2

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

```
{
  "msg": 8
}
```

B.1.1.2 Resposta - mensagem 3

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

```
{
  "res": 0,
  "idDAF": "ughyrcDYBW0zaIGJG3Z6iw",
  "versaoSB": "1.1.2",
  "hashSB": "CV2lZgWH662O6NuY1COMBt0YX3RrelYejwfFBaRtzUM",
  "modelo": "ughyrcDYBW0zaIGJG3Z6iw",
  "cont": 0,
  "cert": "-----BEGIN CERTIFICATE-----\nMIIDZDCCAkwCCQCZptuvvylwxDANBgkqhkiG9w0BAQsFADB0MQswCQ
    YDVQQGEwJC\nUjEXMBUGA1UECAwOU2FudGEgQ2F0YXJpbmExFjAUBgNVBAcMDUZsb3JpYW5vcG9s\naXMxDDAKBgNVBA
    oMA1NFRjEOMAwGA1UECwwFR0VTQUMxFjAUBgNVBAMMDXNlZi5z\nYy5nb3YuYnIwHhcNMjAwOTIzMTYyMDE3WhcNMzAw
    OTIxMTYyMDE3WjB0MQswCQYD\nVQQGEwJCUjEXMBUGA1UECAwOU2FudGEgQ2F0YXJpbmExFjAUBgNVBAcMDUZsb3Jp\n
    YW5vcG9saXMxDDAKBgNVBAoMA1NFRjEOMAwGA1UECwwFR0VTQUMxFjAUBgNVBAMM\nDXNlZi5zYy5nb3YuYnIwggEiM
    A0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDa\nyMjTZDIi7+JcN9t9gD8mHUDaP0byrp0rhQ9po8SkoGVkCOe1ls
```

```
    xmXi5wlY1ZNcV+\nOx+ESTcSCT4DIsNooLwhHNVmi6E93yPySJWf7aoQ57+go6dd1UA9k5Y1H2GznFAX\n77fJ2Ip4Rx
    Gz6UerRaW4luO+4gv2R9Ajxfmm/a08BqBrIznj0PJrWhJzllYe7WeS\newDjvek32PDMmeUOKAp4rD7VHW1sOSnyjBqc
    H4ipdAhZCiYM2rX1jGdFChQ39Vyg\nnOrnjVmIgAvgJKRJg12yJfDxDF77K2DHSyipygW9Ihx8xamebW4sxBvaAYR8+
    ipQ\n1dUT9T//omOMfAwVOEx/AgMBAAEwDQYJKoZIhvcNAQELBQADggEBAMilMrIIMv3d\nwLzNqmsk7/9tk2g5pynYY
    DOtspw83JMwWOsfC8Qaucm+HKIEdPOfGWGomYLFXyYO\nBwZWK1NewcDvrGoQCyxd2NO/lhybwC3q5W3NRzS2seV/OYx
    wczHTrnrCjr1Tmd33\n/AhEqn5dXeKQnqOG1F17mJW4lRlT2FlmlvYmCSyuBUQUtkN8p/mVjsSwOKFgpG4z\nQgGlHaN
    kyje0ThuGA2tW7cxsnWF8I2H/Gt4jB+jsZcDGs5X/oYdFAv5815XVd1Kk\nWSEBltIsc3hhzEan7FEYWRsZQSRi94K7j
    LOPr7EvNjhl9i4k+8IaQXIxuI1oWD54\nLRqC7wlRu3s=\n-----END CERTIFICATE-----",
  "estado": "PRONTO",
  "retidos": ["ok9vTFrhUPYob_x8QzL6I8roxxy7mgQMCXc-0mJEesA","
    SQG9TKLAotGIfDhNFBRn2MKHbj88UdFB71bx3BhkDSo"],
  "algos": [
    {
      "alg": "RS256",
      "len": "2048"
    }
  ]
}
```

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`

```
<iniciarRegistro xmlns="http://www.portalfiscal.inf.br/daf/wsdl/DAFRegistroDispositivo">
  <pedRegistro versao="1.00" xmlns="http://www.portalfiscal.inf.br/daf">
    <infRegistro Id="ughyrcDYBW0zaIGJG3Z6iw">
      <idDAF>ughyrcDYBW0zaIGJG3Z6iw</idDAF>
      <algoritmosDAF>
        <alg>RS256</alg>
        <tamChave>2048</tamChave>
      </algoritmosDAF>
      <cnpjContribuinte>61585866000104</cnpjContribuinte>
      <idPAF>8mX7H4dJ58FmXl8jekZAS889DGxjDEsN0z1TGOK69dM</idPAF>
      <cnpjResponsavel>60658869000150</cnpjResponsavel>
      <idCSRT>1</idCSRT>
    </infRegistro>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><!-- Assinatura --></Signature>
  </pedRegistro>
</iniciarRegistro>
```

B.1.2.2 Retorno - mensagem 5

Na Listagem B.4 é representado o cabeçalho e o conteúdo para a geração do *token* JWT apresentado na Listagem B.5.

Listagem B.4: Cabeçalho e conteúdo do *token* JWT - retorno do método `iniciarRegistro`

```
{
  "typ": "JWT",
  "alg": "RS256"
}
```

```
{
  "nonce": "n7NSeT3B-lIfITmaOh7Rcw"
}
```

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

```
<iniciarRegistroResponse xmlns="http://www.portalfiscal.inf.br/daf/wsdl/DAFRegistroDispositivo">
  <retRegistro versao="1.00" xmlns="http://www.portalfiscal.inf.br/daf">
    <idDAF>ughyrcDYBW0zaIGJG3Z6iw</idDAF>
    <cStat>1000</cStat>
    <xMotivo>Solicitação de pedido recebida com sucesso</xMotivo>
    <tkDesafio>eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJub25jZSI6Im43TlNlVDNCLWxJZklUbWFPaDdSY3ci
    fQ.Ds8lHO1j-u_1IJecMxzl_2TZ4Xc9aA1lfgZa7yAFZpjtNoObkoSbZqb8B3qwcJrAXq97SJIJLsnKP36q2TjDDhPpD
    ozoVq2EndO_Qn9IFbZFPszaaXUx04ze86LXyXln8R-B0f2y3n4ueyMs9lGwf-ihiRgcHSvz3nTtv39-F-M9bHhQ8I9lL
    tUtz47XXzEhjIZPZwj0iH0xgRJdkSNtO7pVbJP6_nY0UTekcYGxlEATkPxmTH4AEcjQ5x8eq5PUDCpXCzXE6wX_cyhNp
    -3uIhghoF9-5RHMerIg4526_nGrMiPDABFvOGiX-xgIO-m43UUyhRKRec3nV624pZhVMg</tkDesafio>
  </retRegistro>
</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`

```
{
  "msg": 1,
  "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJub25jZSI6Im43TlNlVDNCLWxJZklUbWFPaDdSY3cifQ.
    Ds8lHO1j-u_1IJecMxzl_2TZ4Xc9aA1lfgZa7yAFZpjtNoObkoSbZqb8B3qwcJrAXq97SJIJLsnKP36q2TjDDhPpDo
    zoVq2EndO_Qn9IFbZFPszaaXUx04ze86LXyXln8R-B0f2y3n4ueyMs9lGwf-ihiRgcHSvz3nTtv39-F-M9bHhQ8I9l
    LtUtz47XXzEhjIZPZwj0iH0xgRJdkSNtO7pVbJP6_nY0UTekcYGxlEATkPxmTH4AEcjQ5x8eq5PUDCpXCzXE6wX_cy
    hNp-3uIhghoF9-5RHMerIg4526_nGrMiPDABFvOGiX-xgIO-m43UUyhRKRec3nV624pZhVMg"
}
```

B.1.3.2 Resposta - mensagem 8

Na Listagem B.7 é representado o cabeçalho e o conteúdo para a geração do *token* JWT assinado com a chave privada do DAF. A Listagem B.8 representa o cabeçalho e o conteúdo para a geração do *token* JWT assinado com a chave de ateste, apresentado na Listagem B.9, sendo seu conteúdo o *token* JWT gerado a partir da listagem Listagem B.7.

Listagem B.7: Cabeçalho e conteúdo do *token* JWT assinado com a chave privada do DAF - resposta da mensagem `registrar`

```
{
  "typ": "JWT",
  "alg": "RS256",
  "jwk": {
    "kty": "RSA",
    "n": "tXOjVUGk3UJp_jDzsjjdaXqhkq-PiOpcx2pQ352AIs9_denwdOkQamjZfvri9bqAqcLxIj_ZXAEz8rr2FaEh3Q
    jPueMTo6X3G1mtqMfULoRtVxMczWNTdDUL8ZGunMmF1iWkKpMKlCzGEv6LtwjVS4iwHpdm4QJXecxprH99AB-g0Iikzo
    uGIq1I_IxVPDPJ_GDKXhCe-59iSHYNL-HnGIMu3MrKvJ9MnyVLAfgpunoZlGQfkZAAg3j4QlyV-dpp8F58PkkaFIEnNq
    UgQO_3mu8YDephfgkUUStMyUbndiIWnoAiKxExpdTcALcKOYiPAsUwEHUSi8oZpHFcC8XTfQ",
```

```
    "e": "AQAB"
  }
}
{
  "idDAF": "ughyrcDYBWOzaIGJG3Z6iw",
  "cont": 0,
  "nonce": "n7NSeT3B-lIfITmaOh7Rcw"
}
```

Listagem B.8: Cabeçalho e conteúdo do *token* JWT assinado com a chave de ateste - resposta da mensagem `registrar`

```
{
  "typ": "JWT",
  "alg": "RS256",
  "jwk": {
    "kty": "RSA",
    "n": "4080fc42GcispcDdHvsn6qLQscb-rEazslS6UUeDjaJwEpdQuv-2pp1LDA86IqqWJeofcayKgSUMC9XLYsIWw
    RBnVkkYBOQ8t0tOQbrfwcOOmHCmzCJS2_G813frBUfBKOqwOV55VLlv-T61Sfo27PsH7nMevWB8CJ1KpQZnzddnvKN
    yGLQtEYxAzohnbbx0gSatkjfVyKhX4EEvDbPMWJOgNyyJPvkOAVrSSfNhq_lV-qzaivXkRjYtDtGJ4Guww9MR8eh3h
    kyyxmmfOFzATKMT5cHg1kc_RE9udUvkK9EsQh5rr-RF_T_iHkOmyOi_z1sfQDZ3g7wn1ujh_KO7BcSKdfOy_ALb53j
    DMIfGndqvF_Aj2t89fqKVDNph4W3WWpW5oyjDmliZFuTsxNewmNaVC_gcsq5827Kfv_fgjhF1Dewiju41T57SPZCs6
    B9kxKQN-oHlfMzbCF4D3oofV4rzqlndN2qMTXYTcjkosM-rZWKSuk-SdQ5JHTpVoqeCsRnVKGk4YjNk9TTpwCWbvDt
    sSn-GKejoVCXZTsLm5wiN9e8lognWkGlkhYUJHtipdtAvu8qvcH6jUOpr7Ep615ooir1S0SwIZTNphlno4T-C7EBdr
    dKFCz_POUPqR6QgR6UMU5pQ9mA6Gi1Ot4NXflL7soPlhxKrVVh5fEMxER0",
    "e": "AQAB"
  }
}
{
  "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp3ayI6eyJrdHkiOiJSU0EiLCJuIjoidFgwalZVR2szVUpw
    X2pEenNqamRhWHFoa3EtUGlPcGN4MnBRMzUyQUlzOV9kZW53ZE9rUWFtalpmdnJpOWJxQXFjTHhJal9aWEFFejhycjJG
    YUVoM1FqUHVlTVRvNlgzRzFtdHFNZlVMb1J0VnhNY3pXTlRkRFVMOFpHdW5NbUYxaVdrS3BNS2xDekdFdjZMdHdqVlM0
    aXdIcGRtNFFKWGVjeHBySDk5QUItZzBJaWt6b3VHSXExSV9JeFZQRFBKX0dES1hoQ2UtNTlpU0hZTkwtSG5HSU11M01y
    S3ZKOU1ueVZMQWZncHVub1psR1Fma1pBQWczajRRbHlWLWRwcDhGNThQa2thRklFbk5xVWdRMF8zbXU4WURlcGhmZ2tV
    VVN0TXlVYm5kaUlXbm9BaUt4RXhwZFRjQUxjSzBZaVBBc1V3RUhVU2k4b1pwSEZjQzhYVGZRIiwiZSI6IkFRQUIifX0.
    eyJpZERBRiI6InVnaHlyYORZQlcwemFJR0pHM1o2aXciLCJjb250IjowLCJub25jZSI6Im43TlNlVDNCLWxJZklUbWFP
    aDdSY3cifQ.b685PaM1BLbnLnoLrtZNsBz5IU2VXpePgFZOE5w6pihFiigJOhsrfoEwgT6bp-op_muG1-7oUsvKpbt9N
    yHV1FxsSLMOB1FVUJqxrim9DWQIDgTtlW1OcM3mJKwMgW6hHTuFOJRBLB_7cO72A_A4-6SEWhtcaalwjrkn29rer4SI
    M62GZBuSjdxtm3mL74ghaOwFS5av6j4CPNNtH-n47z6tW17mbVDY8vWdQ6FnRFAZedyRDgBndwyEWNiHNjNoVFYjkg93
    zqgs_VOhvQNyM_ZbO5gYeqFQzAwZjLkov8FbxfHslFxJVgKgk5AGVl2MJxvTrokz2v1K1vrVF4quQQ"
}
```

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

```
{
  "res": 0,
  "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp3ayI6eyJrdHkiOiJSU0EiLCJuIjoiNDA4MGZjNDJHY2lz
    cGNEZEh2c242cUxRc2NiLXJFYXpzbFM2VVVlRGphSndFcGRRdXYtMnBwMUxEQTg2SXFxVOplb2ZjYXlLZ1NVTUM5WExZ
    c0lXd1JCblZra1lCMFE4dDBOT1FicmZ3Y09PbUhDbXpDSlMyX0c4MTNmckJVZkJLMHF3MFY1NVZMbHYtVDYxU2ZvMjdQ
    c0g3bk1ldldCOENKMUtwUVpuemRkbnZLTnlHTFFOORVl4QXpvaG5iYngwZ1NhdGtqZlZ5S2hYNEVFdkRiUE1XSjBnTnl5
    S1B2azBBVnJTU2ZOaHFfbFYtcXphaXZYa1JqWXREdEdKNEd1d3c5TVI4ZWgzaGt5eXhtbWZPRnpBVEtNVDVjSGcxa2Nf
    UkU5dWRVdmtLOUVzUWg1cnItUkZfVF9pSGtPbXkwaV96MXNmUURaM2c3d24xdWpoX0tPN0JjU0tkZk95X0FMYjUzakRN
    SWZHbmRxdkZfQWoydDg5ZnFLVkROcGg0VzNXV3BXNW95akRtbG1aRnVUc3hOZXdtTmFWQ19nY3NxNTgyN0tmdl9mZ2po
    RjFEZXdpanU0MVQ1N1NQWkNzNkI5a3hLUU4tb0hsZk16YkNGNEQzb29mVjRyenFsbmROMnFNVFhZVGNqa29zTS1yWldL
```

```
U3VrLVNkUTVKSFRwVm9xZUNzUm5WSOdrNFlqTms5VFRwdONXYnZEdHNTbi1HS2Vqb1ZDWFpUc0xtNXdpTjllOGxvZ25X
aOdsa2hZVUpIdGlwZHRBdnU4cXZjSDZqVU9wcjdFcDYxNW9vaXIxUzBTdOlaVE5waGxubzRULUM3RUJkcmRLRkN6X1Aw
VVBxUjZRZ1I2VU1VNXBROW1BNkdpMU9ONE5YZmxMN3NvUGxoeEtyVlZoNWZFTXhFUjAiLCJlIjoiQVFBQiJ9fQ.eyJqd
3QiOiJleUowZVhBaU9pSktWMVFpTENKaGJHY2lPaUpTVXpJMU5pSXNJbXAzYXlJNmV5SnJkSGtpT2lKU1UwRWlMQOp1S
WpvaWRGZ3dhbFpWUjJzelZVcHdYMnBFZW5OcWFtUmhXSEZvYTNFdFVHbFBjRO40TW5CUk16VXlRVWx6T1Y5a1pXNTNaR
TlyVVdGdGFscG1kbkpwT1dKeFFYRmpUSGhKYWw5YVdFRkZlamh5Y2pKR1lVVm9NMUZxVUhWbFRWUnZObGd6UnpGdGRIR
k5abFZNYjFKMFZuaE5ZM3BYVGxSa1JGVk1PRnBIZFc1TmJVWXhhVmRyUzNCTlMyeERla2RGZGpaTWRIZHFWbEOwYVhkS
WNHUnRORkZLVOdWamVIQnlTRGs1UVVJdFp6QkphV3Q2YjNWSFNYRXhTVjlKZUZaUVJGQktYMGRFUzFob1EyVXROVGxwV
TBoWlRrd3RTRzVIU1UxMUOwMXlTM1pLT1UxdWVWWk1RV1puYOhWdWIxcHNSMUZtYTFwQlFXY3phalJSYkhsV0xXUndjR
GhHTlRoUWEydGhSa2xGYms1eFZXZFJNRjh6YlhVNFdVUmxjR2htWjJOVlZWTjBUWGxWWW01a2FVbFhibTlCYVVONFJYa
HdaRlJqUVV4alN6QlphVkJCYzFWM1JVaFZVMms0YjFwd1NFWmpRemhZVkdaUklpd2laUOk2SWtGUlFVSWlmWDAuZXlKc
FpFUkJSaUk2SW5WbmFIbHlZMFJaUWxjd2VtRkpSMHBITTFvMmFYY2lMQOpqYjI1MElqb3dMQOp1YjI1alpTSTZJbTQzV
GxObFZETkNMV3hKWmtsVWJXRlBhRGRTWTNjaWZRLmI2ODVQYUOxQkxibkxub0xydFpOc0J6NUlVMlZYcGVQZOZaTOU1d
zZwaWhGaWlnSjBoc3Jmb0V3Z1Q2YnAtb3BfbXVHMSO3b1VzdktwYnQ5TnlIVjFGeHNTTEOwQjFGVlVKcXhyaWO5RFdRS
URnVHRsVzFPYOOzbUpLd01nVzZoSFR1Rk9KUkJMQl83Y083MkFfQTQtNlNFV2h0Y2FhbHdqcmtuMjlyZXIOU0lNNjJHW
kJ1U2pkeHRtM21MNzRnaGFPd0ZTNWF2Nmo0Q1BOTnRILW40N3o2dFcxN21iVkRZOHZXZFE2Rm5SRkFaZWR5UkRnQm5kd
3lFV05pSE5qTm9WRllqa2c5M3pxZ3NfVk9odlFOeU1fWmJPNWdZZXFGUXpBd1pqTGtvdjhGYnhmSHNsRnhKVmdLZ2s1Q
UdWbDJNSnh2VHJva3oydjFLMXZyVkYOcXVRUSJ9.AZWkYDlfaNLBHaeWwKOb90t88Nn_XzTdQELQb4_LNYlJFu_EOYA
s5hgyYc78pQlAnFyIx7UIOi9EO2JNJCAVXs7SODluuwgXpw2X1bwJ-QMUwmJONyfsRxgA7RMLGnfadDdA5ba8VOtXoRU
wGRkE4NmOTl8GLewLQiMb2T6TWnlcc_TehtLeNwjS5LUYQJPuyilms6bEbdC_XOpPhVTdtATpVxyeeEgvhXmzGbBxxvJ
IbD4s8LEKYpArvVwwCrP2k6_4Cqdb9sXH-fecyU2LubUvAhsjElV8vao60QM_vQ6nrovIgP5c7iB1TEUp1lAGUGtTJ
j8wSukSvMG1VZUgyEkdyQH53iOtVjyYBncUotLW7ZRa4CUt6WY9Aqtaqxi-pCE5qvQzT8cb6Ko0M2ZRD4zRG-fy1Ogak
jONBSIkwzsTs6O3DSJBHinSPVONUYwdiEO-upGo6EO_Qz_aFFM4-vOzNktuEmoiXjK2NlxO0aaywVPMVVPju68kl8OMn
iRw4Ryq8PUmJbxOQeT2lSnLfOi47xitpfhwHokWsNgGD-3GSb2sXKEwwFteNfAF8gGMde1g9rsN8NYyZbYqpRaL9zxLg
SG43KjzElghfRaJ4hgNiNjVUGebBsqYI2WaqbUA5LPDeuTnlO_c7Uq_8sKOJ53TVfseCPiYSmIEdtZZLGU"
}
```


B.1.4 Serviço SEF `DAFRegistroDispositivo` - método `confirmarRegistro`

B.1.4.1 Entrada - mensagem 9

Listagem B.10: Documento XML de entrada do método `confirmarRegistro`


```
<confirmarRegistro xmlns="http://www.portalfiscal.inf.br/daf/wsdl/DAFRegistroDispositivo">
  <pedConfRegistro versao="1.00" xmlns="http://www.portalfiscal.inf.br/daf">
    <infConfRegistro Id="ughyrcDYBW0zaIGJG3Z6iw">
      <tkAut>eyJOeXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp3ayI6eyJrdHkiOiJSUOEiLCJuIjoiNDA4MGZjNDJH
Y2lzcGNEZEh2c242cUxRc2NiLXJFYXpzbFM2VVVlRGphSndFcGRRdXYtMnBwMUxEQTg2SXFxVOplb2ZjYXlLZ1NVTU
M5WExZcOlXd1JCblZra1lCMFE4dDB0T1FicmZ3YO9PbUhDbXpDSlMyXOc4MTNmckJVZkJLMHF3MFY1NVZMbHYtVDYx
U2ZvMjdQcOg3bk1ldldCOENKMUtwUVpuemRkbnZLTnlHTFFORVl4QXpvaG5iYngwZ1NhdGtqZlZ5S2hYNEVFdkRiU
E1XSjBnTnl5SlB2azBBVnJTU2ZOaHFfbFYtcXphaXZYa1JqWXREdEdKNEd1d3c5TVI4ZWgzaGt5eXhtbWZPRnpBVEt
NVDVjSGcxa2NfUkU5dWRVdmtLOUVzUWg1cnItUkZfVF9pSGtPbXkwaV96MXNmUURaM2c3d24xdWpoXOtPNOJjUOtkZ
k95XOFMYjUzakRNSWZHbmRxdkZfQWoydDg5ZnFLVkROcGgOVzNXV3BXNW95akRtbGlaRnVUc3hOZXdtTmFWQ19nY3N
xNTgyNOtmdl9mZ2poRjFEZXdpanUOMVQ1N1NQWkNzNkI5a3hLUU4tbOhsZk16YkNGNEQzb29mVjRyenFsbmROMnFNV
FhZVGNqa29zTS1yWldLU3VrLVNkUTVKSFRwVm9xZUNzUm5WSOdrNFlqTms5VFRwdONXYnZEdHNTbi1HS2Vqb1ZDWFp
Uc0xtNXdpTjllOGxvZ25Xa0dsa2hZVUpIdGlwZHRBdnU4cXZjSDZqVU9wcjdFcDYxNW9vaXIxUzBTdOlaVE5waGxub
zRULUM3RUJkcmRLRkN6X1AwVVBxUjZRZ1I2VU1VNXBROW1BNkdpMU9ONE5YZmxMN3NvUGxoeEtyVlZoNWZFTXhFUjA
iLCJlIjoiQVFBQiJ9fQ.eyJqd3QiOiJleUowZVhBaU9pSktWMVFpTENKaGJHY2lPaUpTVXpJMU5pSXNJbXAzYXlJNm
V5SnJkSGtpT2lKU1UwRWlMQOp1SWpvaWRGZ3dhbFpWUjJzelZVcHdYMnBFZW5OcWFtUmhXSEZvYTNFdFVHbFBjRO40T
W5CUk16VXlRVWx6T1Y5a1pXNTNaRTlyVVdGdGFscG1kbkpwT1dKeFFYRmpUSGhKYWw5YVdFRkZlamh5Y2pKR1lVVm9N
MUZxVUhWbFRWUnZObGd6UnpGdGRIRk5abFZNYjFKMFZuaE5ZM3BYVGxSa1JGVk1PRnBIZFc1TmJVWXhhVmRyUzNCTl
MyeERla2RGZGpaTWRIZHFWbEOwYVhkSWNHUnRORkZLVOdWamVIQnlTRGs1UVVJdFp6QkphV3Q2YjNWSFNYRXhTVjlK
ZUZaUVJGQktYMGRFUzFob1EyVXROVGxwVTBoWlRrd3RTRzVIU1UxMUOwMXlTM1pLT1UxdWVWWk1RV1puYOhWdWIxcH
NSMUZtYTFwQlFXY3phalJSYkhsV0xXUndjRGhHTlRoUWEydGhSa2xGYms1eFZXZFJNRjh6YlhVNFdVUmxjR2htWjJOVl
```

```
    ZWTjBUWGxWWW01a2FVbFhibTlCYVV0NFJYaHdaRlJqUVV4alN6QlphVkJCYzFWM1JVaFZVMms0YjFwd1NFWmpRemhZV
    kdaUklpd2laU0k2SWtGUlFVSWlmWDAuZXlKcFpFUkJSaUk2SW5WbmFIbHlZMFJaUWxjd2VtRkpSMHBITTFvMmFYY2lM
    Q0pqYjI1MElqb3dMQ0p1YjI1alpTSTZJbTQzVGxObFZETkNMV3hKWmtsVWJXRlBhRGRTWTNjaWZRLmI2ODVQYU0xQkx
    ibkxub0xydFpOc0J6NUlVMlZYcGVQZOZaT0U1dzZwaWhGaWlnSjBoc3Jmb0V3Z1Q2YnAtb3BfbXVHMS03b1VzdktwYn
    Q5TnlIVjFGeHNTTE0wQjFGVlVKcXhyaW05RFdRSURnVHRsVzFPY00zbUpLd01nVzZoSFR1Rk9KUkJMQl83Y083MkFfQ
    TQtNlNFV2h0Y2FhbHdqcmtuMjlyZXIOU0lNNjJHWkJ1U2pkeHRtM21MNzRnaGFPd0ZTNWF2Nmo0Q1BOTnRILW40N3o2d
    FcxN21iVkRZOHZXZFE2Rm5SRkFaZWR5UkRnQm5kd3lFV05pSE5qTm9WRllqa2c5M3pxZ3NfVk9odlFOeU1fWmJPNWdZZ
    XFGUXpBd1pqTGtvdjhGYnhmSHNsRnhKVmdLZ2s1QUdWbDJNSnh2VHJva3oydjFLMXZyVkY0CAVXs7SODluuwgXpw2X1b
    wJ-QMUwmJ0NyfsRxgA7RMLGnfadDdA5ba8V0tXoRUwGRkE4NmOTl8GLewLQiMb2T6TWnlcc_TehtLeNwjS5LUYQJPuy
    ilms6bEbdC_X0pPhVTdtATpVxyeeEgvhXmzGbBxxvJIbD4s8LEKYpArvVwwCrP2k6_4Cqdb9sXH-fecyU2LubUvAhsj
    ElV8vao60QM_vQ6nrovIgP5c7iB1TEUp1lAGUGtTJj8wSukSvMG1VZUgyEkdyQH53i0tVjyYBncUotLW7ZRa4CUt6W
    Y9Aqtaqxi-pCE5qvQzT8cb6Ko0M2ZRD4zRG-fy10gakj0NBSIkwzsTs6O3DSJBHinSPVONUYwdiEO-upGo6E0_Qz_aF
    FM4-vOzNktuEmoiXjK2NlxO0aaywVPMVVPju68kl8OMniRw4Ryq8PUmJbxOQeT2lSnLfOi47xitpfhwHokWsNgGD-3G
    Sb2sXKEwwFteNfAF8gGMde1g9rsN8NYyZbYqpRaL9zxLgSG43KjzElghfRaJ4hgNiNjVUGebBsqYI2WaqbUA5LPDeuT
    nlO_c7Uq_8sK0J53TVfseCPiYSmIEdtZZLGU</tkAut>
      <idDAF>ughyrcDYBW0zaIGJG3Z6iw</idDAF>
      <idPAF>8mX7H4dJ58FmXl8jekZAS889DGxjDEsN0z1TGOK69dM</idPAF>
    </infConfRegistro>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><!-- Assinatura --></Signature>
  </pedConfRegistro>
</confirmarRegistro>
```


B.1.4.2 Retorno - mensagem 11

Na Listagem B.11 é representado o cabeçalho e o conteúdo para a geração do *token* JWT apresentado na Listagem B.12.

Listagem B.11: Cabeçalho e conteúdo do *token* JWT - retorno do método `confirmarRegistro`


```
{
  "typ": "JWT",
  "alg": "RS256"
}
{
  "chSEF": "W0JxjN10Z2fUQnz6dAqRK0YQaCoh1ak6NP3yUlBsSOJBFVaGUfU34zWoTM_eZfRM2endpEcQ_rlQBXsjVS
    tHn2jnfzlDt3zo_s5XblCvIHFxoEKmHuSMMk3WL3Vb86mtC4dHwU4sZmGgUoaMiDwqEHn_BcAs98xZvqioHDPWF8wO9
    yd7C7xugudzffWXUe6nlggCMjFADwLo xDIXebVgs1AjgH0aL9qn2sy1lJZ9_cOMQg2Sn4Wdg7_O6g",
  "chPAF": "yUAKi4B4NTy4KFLmHX-B70wOpbZfPtt3ijLBEtHJOwJVFCEawjzpL4mLKMHAWsI37HkzBJ2OVf2hFkpbjE
    B7ig"
}
```


Listagem B.12: Documento XML de retorno do método `confirmarRegistro`


```
<confirmarRegistroResponse xmlns="http://www.portalfiscal.inf.br/daf/wsdl/DAFRegistroDispositivo">
  <retConfRegistro versao="1.00" xmlns="http://www.portalfiscal.inf.br/daf">
    <idDAF>ughyrcDYBW0zaIGJG3Z6iw</idDAF>
    <cStat>1001</cStat>
    <xMotivo> Dispositivo registrado com sucesso</xMotivo>
    <tkChaves>eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJjaFNFRiI6IlcwSnhqTjEwWjJmVVFuejZkQXF
    SSzBZUWFDb2gxYWs2TlAzeVVsQnNTT0pCRlZhR1VmVTM0eldvVE1fZVpmUk0yZW5kcEVjUV9ybFFCWHNqVlNOSG4ya
    m5memxEdDN6b19zNVhibEN2SUhGeG9FS21IdVNNTWszV0wzVmI4Nm10QzRkSHdVNHNabUdnVW9hTWlEd3FFSG5fQmN
    Bczk4eFp2cWlvSERQV0Y4d085eU9TY3lnNXo1aHNxaC1qQmZTTU1SQjZialh3alR0V2pGNjVuM1ZPX2dhSVFKV1IzY
    WtzNHQ2MTA4aGIwY3dCeFdfSzJsQlFta2dLRXlPZ3BOUk9LZW5YT1VyMkk0ZDdDN3h1Z3VkemZmV1hVZTZubGdnQ01
```

```
    qRkFEd0xveERJWGViVmdzMUFqZ0gwYUw5cW4yc3kxbEpaOV9jT01RZzJTbjRXZGc3X082ZyIsImNoUEFGIjoieVVBS2
    k0QjROVHk0S0ZMbUhYLUI3MHdPcGJaZlB0dDNpakxCRXRISk93SlZGQ0Vhd2p6cEw0bUxLTUhBV3NJMzdIa3pCSjJP
    VmYyaEZrcGJqRUI3aWcifQ.r0nk0RKQ5r8PkInDxjcvxzvjqwCmX-Megw5KUOVvn7EhA7mOos2Oiutd2IFq530RznI6
    DnWXxKQrkaS77YWxGuZx-SMqPQqgL5NjfJhWUeGNwUTlLEe09rzTcJ9Kk7Qr_pv-VRSK3jDWdhA2jUSaL3Z5DErCT4
    Xih23V2b3V69KxYa4TrJVk6d6azmbDqh0RoDjqFQG29UYdo49IaNCFrwPfD4Flj-XW3k6898Ve80YcRPYhHeagN_By
    hlXAB0XSliWkV0gfxNCK_ZWPMjhvKThdGFv-Eigc-c13J4-vo1T0Ulvkqhz2TutqjnJX8QgjFKVd32pxEMyCpKsgAS
    sIbg</tkChaves>
  </retConfRegistro>
</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`

```
{
  "msg": 2,
  "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJjaFNFRiI6IlcwSnhqTjEwWjJmVVFuejZkQXFSSzBZUWF
    Db2gxYWs2TlAzeVVsQnNTT0pCRlZhR1VmVTM0eldvVE1fZVpmUk0yZW5kcEVjUV9ybFFCWHNqVlNOSG4yam5memxEdDN
    6b19zNVhibEN2SUhGeG9FS21IdVNNTWszV0wzVmI4Nm10QzRkSHdVNHNabUdnVW9hTWlEd3FFSG5fQmNBczk4eFp2cWl
    vSERQV0Y4d085eU9TY3lnNXo1aHNxaC1qQmZTTU1SQjZialh3alR0V2pGNjVuM1ZPX2dhSVFKV1IzYWtzNHQ2MTA4aGI
    wY3dCeFdfSzJsQlFta2dLRXlPZ3BOUk9LZW5YT1VyMkk0ZDdDN3h1Z3VkemZmV1hVZTZubGdnQ01qRkFEd0xveERJWGV
    iVmdzMUFqZ0gwYUw5cW4yc3kxbEpaOV9jT01RZzJTbjRXZGc3X082ZyIsImNoUEFGIjoieVVBS2k0QjROVHk0S0ZMbUh
    YLUI3MHdPcGJaZlB0dDNpakxCRXRISk93SlZGQ0Vhd2p6cEw0bUxLTUhBV3NJMzdIa3pCSjJPVmYyaEZrcGJqRUI3aWc
    ifQ.r0nk0RKQ5r8PkInDxjcvxzvjqwCmX-Megw5KUOVvn7EhA7mOos2Oiutd2IFq530RznI6DnWXxKQrkaS77YWxGuZx-
    SMqPQqgL5NjfJhWUeGNwUTlLEe09rzTcJ9Kk7Qr_pv-VRSK3jDWdhA2jUSaL3Z5DErCT4Xih23V2b3V69KxYa4TrJVk6
    d6azmbDqh0RoDjqFQG29UYdo49IaNCFrwPfD4Flj-XW3k6898Ve80YcRPYhHeagN_ByhlXAB0XSliWkV0gfxNCK_ZWP
    MjhvKThdGFv-Eigc-c13J4-vo1T0Ulvkqhz2TutqjnJX8QgjFKVd32pxEMyCpKsgASsIbg"
}
```

B.1.5.2 Resposta - mensagem 14

Listagem B.14: Documento JSON para a resposta da mensagem `confirmarRegistro`

```
{
  "res": 0
}
```

B.2 Remover registro do DAF junto à SEF

Os exemplos apresentados referem-se as mensagens ilustradas no diagrama de sequência apresentado na Figura 5.7. O processo operacional é detalhado na Seção 5.4 e fluxos alternativos e de exceção para esse processo são apresentados nos Casos de Uso UC-4.11 e UC-4.1.

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`

```xml
<removerRegistro xmlns="http://www.portalfiscal.inf.br/daf/wsdl/DAFRemocaoRegistro">
  <pedRemRegistro versao="1.00" xmlns="http://www.portalfiscal.inf.br/daf">
    <infRemRegistro Id="ughyrcDYBW0zaIGJG3Z6iw">
      <idDAF>ughyrcDYBW0zaIGJG3Z6iw</idDAF>
      <idPAF>8mX7H4dJ58FmXl8jekZAS889DGxjDEsN0z1TGOK69dM</idPAF>
      <xJust>Motivo do pedido de remoção do registro</xJust>
    </infRemRegistro>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><!-- Assinatura --></Signature>
  </pedRemRegistro>
</removerRegistro>
```

B.2.1.2 Retorno - mensagem 3

Na Listagem B.16 é representado o cabeçalho e o conteúdo para a geração do *token* JWT apresentado na Listagem B.17.

Listagem B.16: Cabeçalho e conteúdo do *token* JWT - retorno do método `removerRegistro`

```json
{
  "typ": "JWT",
  "alg": "RS256"
}
{
  "nonce": "n7NSeT3B-lIfITmaOh7Rcw"
}
```

Listagem B.17: Documento XML de retorno do método `removerRegistro`

```xml
<removerRegistroResponse xmlns="http://www.portalfiscal.inf.br/daf/wsdl/DAFRemocaoRegistro">
  <retRemRegistro versao="1.00" xmlns="http://www.portalfiscal.inf.br/daf">
    <idDAF>ughyrcDYBW0zaIGJG3Z6iw</idDAF>
    <cStat>1000</cStat>
    <xMotivo>Solicitação de pedido recebida com sucesso</xMotivo>
    <tkDesafio>eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJub25jZSI6Im43TlNlVDNCLWxJZklUbWFPaDdSY3
    cifQ.Ds8lHO1j-u_1IJecMxzl_2TZ4Xc9aA1lfgZa7yAFZpjtNoObkoSbZqb8B3qwcJrAXq97SJIJLsnKP36q2TjDD
    hPpDozoVq2EndO_Qn9IFbZFPszaaXUx04ze86LXyXln8R-B0f2y3n4ueyMs9lGwf-ihiRgcHSvz3nTtv39-F-M9bHh
    Q8I9lLtUtz47XXzEhjIZPZwj0iH0xgRJdkSNtO7pVbJP6_nYOUTekcYGxlEATkPxmTH4AEcjQ5x8eq5PUDCpXCzXE6
    wX_cyhNp-3uIhghoF9-5RHMerIg4526_nGrMiPDABFvOGiX-xgIO-m43UUyhRKRec3nV624pZhVMg</tkDesafio>
  </retRemRegistro>
</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`

```json
{
  "msg": 6,
  "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJub25jZSI6Im43TlNlVDNCLWxJZklUbWFPaDdSY3cifQ.
    Ds8lHO1j-u_1IJecMxzl_2TZ4Xc9aA1lfgZa7yAFZpjtNoObkoSbZqb8B3qwcJrAXq97SJIJLsnKP36q2TjDDhPpDozo
```

```
    Vq2EndO_Qn9IFbZFPszaaXUx04ze86LXyXln8R-BOf2y3n4ueyMs9lGwf-ihiRgcHSvz3nTtv39-F-M9bHhQ8I9lLtUt
    z47XXzEhjIZPZwj0iH0xgRJdkSNtO7pVbJP6_nY0UTekcYGxlEATkPxmTH4AEcjQ5x8eq5PUDCpXCzXE6wX_cyhNp-3u
    IhghoF9-5RHMerIg4526_nGrMiPDABFvOGiX-xgIO-m43UUyhRKRec3nV624pZhVMg"
}
```

B.2.2.2 Resposta - mensagem 6

Na Listagem B.19 é representado o cabeçalho e o conteúdo para a geração do *token* JWT apresentado na Listagem B.20.

Listagem B.19: Cabeçalho e conteúdo do *token* JWT - resposta da mensagem `removerRegistro`

```
{
  "typ": "JWT",
  "alg": "RS256"
}
{
  "idDAF": "ughyrcDYBW0zaIGJG3Z6iw",
  "cont": 0,
  "nonce": "n7NSeT3B-lIfITmaOh7Rcw"
}
```

Listagem B.20: Documento JSON para a resposta da mensagem `removerRegistro`

```
{
  "res": 0,
  "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJpZERBRiI6InVnaHlyY0RZQlcwemFJR0pHM1o2aXciLCJ
    jb250IjowLCJub25jZSI6Im43TlNlVDNCLWxJZklUbWFPaDdSY3cifQ.hBN3EgDax9iuiyX_2wFIlsBeaqB4G32DF4M2
    sp6rta_8Eq-t1I8MkEDuqQ6lKhcVhdlStzLBdNiFmWzXKXL6rIvYwdNFmF8rDqaPse_maHzCFDVMbnhVLwBuvgwUxYii
    n-YyNjsik6-IJSOGJYc5E9-f1i9xhFMP6Cx2RDZqkilLxiOlofGQITPhOVyuLNN9du8lIdWjh_oLYXqsZPMbDINXOc4d
    CkjNApFJvCN3WpFh9UAwptkxQJ7sUeBkttZk27LwF6El6ZwdQeI5dJcnbfc9gJeS7YNat1wBxBMdA3TascyFrM4fMSfL
    oVRC_LoCH4Jt9du3Hpnegc_FYpx_SA"
}
```

B.2.3 Serviço SEF `DAFRemocaoRegistro` - método `confirmarRemoverRegistro`

B.2.3.1 Entrada - mensagem 7

Listagem B.21: Documento XML de entrada do método `confirmarRemoverRegistro`

```
<confirmarRemoverRegistro xmlns="http://www.portalfiscal.inf.br/daf/wsdl/DAFRemocaoRegistro">
  <pedConfRemRegistro versao="1.00" xmlns="http://www.portalfiscal.inf.br/daf">
    <infConfRemRegistro Id="ughyrcDYBW0zaIGJG3Z6iw">
      <tkAut>eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJpZERBRiI6InVnaHlyY0RZQlcwemFJR0pHM1o2aXci
    LCJjb250IjowLCJub25jZSI6Im43TlNlVDNCLWxJZklUbWFPaDdSY3cifQ.hBN3EgDax9iuiyX_2wFIlsBeaqB4G32D
    F4M2sp6rta_8Eq-t1I8MkEDuqQ6lKhcVhdlStzLBdNiFmWzXKXL6rIvYwdNFmF8rDqaPse_maHzCFDVMbnhVLwBuvg
    wUxYiin-YyNjsik6-IJSOGJYc5E9-f1i9xhFMP6Cx2RDZqkilLxiOlofGQITPhOVyuLNN9du8lIdWjh_oLYXqsZPMb
    DINXOc4dCkjNApFJvCN3WpFh9UAwptkxQJ7sUeBkttZk27LwF6El6ZwdQeI5dJcnbfc9gJeS7YNat1wBxBMdA3Tasc
    yFrM4fMSfLoVRC_LoCH4Jt9du3Hpnegc_FYpx_SA</tkAut>
      <idDAF>ughyrcDYBW0zaIGJG3Z6iw</idDAF>
      <idPAF>8mX7H4dJ58FmXl8jekZAS889DGxjDEsNOz1TGOK69dM</idPAF>
    </infConfRemRegistro>
```

```
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><!-- Assinatura --></Signature>
  </pedConfRemRegistro>
</confirmarRemoverRegistro>
```

B.2.3.2 Retorno - mensagem 8

Na Listagem B.22 é representado o cabeçalho e o conteúdo para a geração do *token* JWT apresentado na Listagem B.23.

Listagem B.22: Cabeçalho e conteúdo do *token* JWT - retorno do método `confirmarRemoverRegistro`

```
{
  "typ": "JWT",
  "alg": "RS256"
}
{
  "evento": "REMOVER"
}
```

Listagem B.23: Documento XML de retorno do método `confirmarRemoverRegistro`

```
<confirmarRemoverRegistroResponse xmlns="http://www.portalfiscal.inf.br/daf/wsdl/
    DAFRemocaoRegistro">
  <retConfRemRegistro versao="1.00" xmlns="http://www.portalfiscal.inf.br/daf">
    <idDAF>ughyrcDYBW0zaIGJG3Z6iw</idDAF>
    <cStat>1002</cStat>
    <xMotivo>Registro de dispositivo removido</xMotivo>
    <tkEvento>eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJldmVudG8iOiJSRU1PVkVSIn0.mYdPi0Q1uD4P-by0
    drwnDFF-QsU0Bq6KVcRvdowLjtzJdH0FlgIOLRabitf3FXu0sBAQwCJh7KrlKHAxg_TxNn3dgSuY-JoRWaxxy-Cib
    siIoAoO3CREwEu-dLHUI9CqjpQiaXhxN62GS8h55pZq6j1F7GZmMoW1YsPJy9NaV799-fB0mK5k3z-wrHB_nyngSKX
    Fmv1IZBibcRI6WvOgsm5qFFsA8L87P4-G0WyDlFH8TObpPrI6H8zol4DRTDHmuycDqKxyWx5sLuWCH6xthBV9Qh43V
    iQbdu2wWCLYCDN3UoA7-4_-jnAawF2zaEGtc_VKkir_J7pVI2x_XoEJIA</tkEvento>
  </retConfRemRegistro>
</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`

```
{
  "msg": 7,
  "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJldmVudG8iOiJSRU1PVkVSIn0.mYdPi0Q1uD4P-by0drw
    nDFF-QsU0Bq6KVcRvdowLjtzJdH0FlgIOLRabitf3FXu0sBAQwCJh7KrlKHAxg_TxNn3dgSuY-JoRWaxxy-CibsiIoA
    oO3CREwEu-dLHUI9CqjpQiaXhxN62GS8h55pZq6j1F7GZmMoW1YsPJy9NaV799-fB0mK5k3z-wrHB_nyngSKXFmv1IZB
    ibcRI6WvOgsm5qFFsA8L87P4-G0WyDlFH8TObpPrI6H8zol4DRTDHmuycDqKxyWx5sLuWCH6xthBV9Qh43ViQbdu2wWC
    LYCDN3UoA7-4_-jnAawF2zaEGtc_VKkir_J7pVI2x_XoEJIA"
}
```

B.2.4.2 Resposta - mensagem 11

Listagem B.25: Documento JSON para a resposta da mensagem `confirmarRemocaoRegistro`

```
{
  "res": 0
}
```

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-4.5, UC-4.2 e UC-4.7.

B.3.1 Mensagem DAF `solicitarAutenticacao`

B.3.1.1 Pedido - mensagem 2

Listagem B.26: Documento JSON para o pedido da mensagem `solicitarAutenticacao`

```
{
  "msg": 3
}
```

B.3.1.2 Resposta - mensagem 3

Listagem B.27: Documento JSON para a resposta da mensagem `solicitarAutenticacao`

```
{
  "res": 0,
  "nonce": "n7NSeT3B-lIfITmaOh7Rcw"
}
```

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`

```
<infNFe Id="NFe42200861585866000104650008024522711130900054" versao="4.00"><ide><cUF>42</cUF><cNF>
    13090005</cNF><natOp>VENDA DE MERCADORIA CONFORME CFOP</natOp><mod>65</mod><serie>0</serie><
    nNF>802452271</nNF><dhEmi>2020-08-19T13:38:04-03:00</dhEmi><tpNF>1</tpNF><idDest>1</idDest><
    cMunFG>4205407</cMunFG><tpImp>5</tpImp><tpEmis>1</tpEmis><cDV>4</cDV><tpAmb>1</tpAmb><finNFe>1
    </finNFe><indFinal>1</indFinal><indPres>1</indPres><procEmi>0</procEmi><verProc>NFC-e
    1.0.41.00Ce</verProc></ide><emit><CNPJ>61585866000104</CNPJ><xNome>NOME DO ESTABELECIMENTO
    COMERCIAL</xNome><enderEmit><xLgr>RUA</xLgr><nro>999</nro><xCpl>SALA 1</xCpl><xBairro>BAIRRO</
    xBairro><cMun>4205407</cMun><xMun>Florianópolis</xMun><UF>SC</UF><CEP>88010000</CEP><cPais>
```

```
1058</cPais><xPais>BRASIL</xPais><fone>9999999999</fone></enderEmit><IE>9999999999</IE><CRT>1<
/CRT></emit><dest><CPF>53939762083</CPF><xNome>nome do cliente</xNome><indIEDest>9</indIEDest>
<email>email@cliente.com</email></dest><det nItem="1"><prod><cProd>PI3199</cProd><cEAN>SEM
GTIN</cEAN><xProd>NOME DO PRODUTO</xProd><NCM>70099200</NCM><CEST>1008000</CEST><CFOP>5405</
CFOP><uCom>UN</uCom><qCom>1.0000</qCom><vUnCom>229.9000000000</vUnCom><vProd>229.90</vProd><
cEANTrib>SEM GTIN</cEANTrib><uTrib>UN</uTrib><qTrib>1.0000</qTrib><vUnTrib>229.9000</vUnTrib><
indTot>1</indTot></prod><imposto><vTotTrib>87.64</vTotTrib><ICMS><ICMSSN500><orig>1</orig><
CSOSN>500</CSOSN></ICMSSN500></ICMS><PIS><PISNT><CST>08</CST></PISNT></PIS><COFINS><COFINSNT><
CST>08</CST></COFINSNT></COFINS></imposto></det><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><transp><modFrete>9</modFrete></transp><pag><detPag><tPag>03</tPag><vPag>
229.90</vPag><card><tpIntegra>2</tpIntegra><CNPJ>01027058000191</CNPJ><tBand>02</tBand><cAut>
6c933785</cAut></card></detPag></pag><infAdic><infCpl>Trib. Aprox. R$ 46,26 Federal e 41,38
Estadual e 0,00 Municipal Fonte: IBPT/empresometro.com.br 5A16F8------</infCpl></infAdic><
infRespTec><CNPJ>49443706000117</CNPJ><xContato>nome do responsável</xContato><email>
email@responsavel.com</email><fone>9999999999</fone></infRespTec></infNFe>
```


Listagem B.29: Fragmento XML com conjunto de informações essenciais de uma NFC-e para o pedido da mensagem `autorizarDFE`


```
<infNFe Id="NFe42200861585866000104650008024522711130900054" versao="4.00"><ide><cUF>42</cUF><cNF>
13090005</cNF><natOp>VENDA DE MERCADORIA CONFORME CFOP</natOp><mod>65</mod><serie>0</serie><
nNF>802452271</nNF><dhEmi>2020-08-19T13:38:04-03:00</dhEmi><tpNF>1</tpNF><idDest>1</idDest><
cMunFG>4205407</cMunFG><tpImp>5</tpImp><tpEmis>1</tpEmis><cDV>4</cDV><tpAmb>1</tpAmb><finNFe>1
</finNFe><indFinal>1</indFinal><indPres>1</indPres><procEmi>0</procEmi><verProc>NFC-e
1.0.41.00Ce</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`


```
{
  "msg": 4,
  "fragDFE": "PGluZk5GZSBJZDOiTkZlNDIyMDA4NjE1ODU4NjYwMDAxMDQ2NTAwMDgwMjQ1MjI3MTExMzA5MDAwNTQi
    IHZlcnNhbzOiNC4wMCI-PGlkZT48Y1VGPjQyPC9jVUY-PGNORj4xMzA5MDAwNTwvYO5GPjxuYXRPcD5WRU5EQSBERSBN
    RVJDQURPUklBIENPTkZPUk1FIENGT1A8L25hdE9wPjxtb2Q-NjU8L21vZD48c2VyaWU-MDwvc2VyaWU-PG5ORj44MDIO
    NTIyNzE8L25ORj48ZGhFbWk-MjAyMCOwOCOxOVQxMzozODowNCOwMzowMDwvZGhFbWk-PHRwTkY-MTwvdHBORj48aWRE
    ZXNOPjE8L2lkRGVzdD48YO11bkZHPjQyMDUOMDc8L2NNdW5GRz48dHBJbXA-NTwvdHBJbXA-PHRwRW1pcz4xPC90cEVt
    aXM-PGNEVj4OPC9jRFY-PHRwQW1iPjE8L3RwQW1iPjxmaW5ORmU-MTwvZmluTkZlPjxpbmRGaW5hbD4xPC9pbmRGaW5h
    bD48aW5kUHJlcz4xPC9pbmRQcmVzPjxwcm9jRW1pPjA8L3Byb2NFbWk-PHZlclByb2M-TkZDLWUgMS4wLjQxLjAwQ2U8
    L3ZlclByb2M-PC9pZGU-PHRvdGFsPjxJQO1TVG9OPjx2QkM-MC4wMDwvdkJDPjx2SUNNUz4wLjAwPC92SUNNUz48dklD
    TVNEZXNvbj4wLjAwPC92SUNNUORlc29uPjx2RkNQPjAuMDA8L3ZGQ1A-PHZCQ1NUPjAuMDA8L3ZCQ1NUPjx2U1Q-MC4w
    MDwvdlNUPjx2RkNQU1Q-MC4wMDwvdkZDUFNUPjx2RkNQU1RSZXQ-MC4wMDwvdkZDUFNUUmVOPjx2UHJvZD4yMjkuOTA8
    L3ZQcm9kPjx2RnJldGU-MC4wMDwvdkZyZXRlPjx2U2VnPjAuMDA8L3ZTZWc-PHZEZXNjPjAuMDA8L3ZEZXNjPjx2SUk-
    MC4wMDwvdklJPjx2SVBJPjAuMDA8L3ZJUEk-PHZJUElEZXZvbD4wLjAwPC92SVBJRGV2b2w-PHZQSVM-MC4wMDwvdlBJ
    Uz48dkNPRklOUz4wLjAwPC92Q09GSU5TPjx2T3V0cm8-MC4wMDwvdk91dHJvPjx2TkY-MjI5LjkwPC92TkY-PHZUb3RU
    cmliPjg3LjY0PC92VG90VHJpYj48L0lDTVNUb3Q-PC90b3RhbD48L2luZk5GZT4",
  "hashDFE": "fwUV7diyXoDqM-vqShFKYWxtaWjeoGc1ZGD7L8OmHoA",
```

```
  "respDes": "mgz4EkN3hfCdqW0_Iwchc5wW5kN2z0JJHKypazbopBM"
}
```

B.3.2.2 Resposta - mensagem 6

Na Listagem B.31 é representado o cabeçalho e o conteúdo para a geração do *token* JWT apresentado na Listagem B.32.

Listagem B.31: Documento JSON para a resposta da mensagem `autorizarDFE`

```
{
  "typ": "JWT",
  "alg": "HS256"
}
{
  "idDAF": "ughyrcDYBW0zaIGJG3Z6iw",
  "cont": 0,
  "versaoSB": "1.1.2",
  "idAut": "Sw9b-TJua-qypYlKv0yB6SSMnkObo_azJOq1cqzfED0"
}
```

Listagem B.32: Documento JSON para a resposta da mensagem `autorizarDFE`

```
{
  "res": 0,
  "jwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpZERBRiI6InVnaHlyY0RZQlcwemFJR0pHM1o2aXciL
    CJjb250IjowLCJ2ZXJzYW9TQiI6IjEuMS4yIiwiaWRBdXQiOiJTdzliLVRKdWEtcXlwWWxLdjB5QjZTU01ua09ib19
    hekpPcTFjcXpmRUQwIn0.Ju1LjDoTqd7sHkbZPC2Ye7U-IzX7zsww4X5BgbRlga4"
}
```

B.4 Apagar autorizações retidas no DAF

Os exemplos apresentados referem-se as mensagens ilustradas no diagrama de sequência apresentado na Figura 5.5. O processo operacional é detalhado na Seção 5.3 e fluxos alternativos e de exceção para esse processo são apresentados no Caso de Uso UC-4.1.

B.4.1 Serviço SEF `DAFResultadoAutorizacao` - método `obterResultadoAutorizacao`

B.4.1.1 Entrada - mensagem 2

Listagem B.33: Documento XML de entrada do método `obterResultadoAutorizacao`

```
<obterResultadoAutorizacao xmlns="http://www.portalfiscal.inf.br/daf/wsdl/DAFResultadoAutorizacao"
    >
  <pedAutorizacao versao="1.00" xmlns="http://www.portalfiscal.inf.br/daf">
    <infAutorizacao Id="ughyrcDYBW0zaIGJG3Z6iw">
      <idDAF>ughyrcDYBW0zaIGJG3Z6iw</idDAF>
      <idPAF>8mX7H4dJ58FmXl8jekZAS889DGxjDEsN0z1TGOK69dM</idPAF>
      <chDFe>42200861585866000104650008024522711130900054</chDFe>
    </infAutorizacao>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><!-- Assinatura --></Signature>
```

```
  </pedAutorizacao>
</obterResultadoAutorizacao>
```

B.4.1.2 Retorno - mensagem 3

Listagem B.34: Documento XML de retorno do método `obterResultadoAutorizacao`

```
<obterResultadoAutorizacaoResponse xmlns="http://www.portalfiscal.inf.br/daf/wsdl/
    DAFResultadoAutorizacao">
  <retAutorizacao versao="1.00" xmlns="http://www.portalfiscal.inf.br/daf">
    <idDAF>ughyrcDYBW0zaIGJG3Z6iw</idDAF>
    <cStat>1000</cStat>
    <xMotivo>Solicitação de pedido recebida com sucesso</xMotivo>
    <retDFe>
      <idAut>ok9vTFrhUPYob_x8QzL6I8roxxy7mgQMCXc-0mJEesA</idAut>
      <hAut>Vb-gMi4xp_sE0VBxP9b39GvaoRUVV7JzURmSjf3zgM8</hAut>
      <chDFe>42200861585866000104650008024522711130900054</chDFe>
      <cStatAut>1005</cStatAut>
      <xMotAut>Validação do fragmento DAF realizada com sucesso</xMotAut>
    </retDFe>
  </retAutorizacao>
</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`

```
{
  "msg": 5,
  "idAut": "ok9vTFrhUPYob_x8QzL6I8roxxy7mgQMCXc-0mJEesA",
  "autApag": "Vb-gMi4xp_sE0VBxP9b39GvaoRUVV7JzURmSjf3zgM8"
}
```

B.4.2.2 Resposta - mensagem 6

Listagem B.36: Documento JSON para a resposta da mensagem `apagarAutorizacaoRetida`

```
{
  "res": 0
}
```