Agência para a Modernização Administrativa I.P.

Serviço de Assinatura de Faturas Eletrónicas

Documento de Integração

Versão 2.1

AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA

Referências a outros Documentos

Ref.	Descrição	Autor
Ref1	Autenticação.Gov - Manual de Integração	AMA
Ref2	Guia rápido de utilização do OAuth2 do FA	AMA
Ref3	Architectures and protocols for remote signature applications – Published version 1.0.4.0 (2019-06)	Cloud Signature Consortium
Ref4	SAFE – Guias de Fluxos Complementares	AMA

Registo de Revisões

Data	Versão	Descrição	Autor
03-09-2020	0.9	Documento Inicial	Tiago Brás
11-09-2020	1.0	Documento Inicial Revisto	André Vasconcelos
06-10-2020	1.1	Revisão dados criação de conta	Tiago Brás
21-10-2020	1.2	Revisão dados criação de conta	Tiago Brás
18-11-2020	1.3	Adição de referência a fluxos complementares e a possíveis respostas de criação de conta, alteração de headers de autorização	Tiago Brás
22-02-2021	1.4	Alteração nome do atributo do SCAP e esclarecimentos	Tiago Brás
01-03-2021	1.5	Correção código de erro de expiração de tokens e esclarecimentos	Tiago Brás
03-03-2022	1.6	Alteração de processo de integração e esclarecimentos	Tiago Brás
11-11-2022	2.0	Atualização de serviços de assinatura	Tiago Brás
03-05-2024	2.1	Atualização informação ativação de conta de assinatura e certificados	

Índice

1 INTRODUÇÃO 5

1.1 DEFINIÇÕES, ACRÓNIMOS E ABREVIAÇÕES 6

2 ARQUITETURA DA SOLUÇÃO 7

3 REQUISITOS PARA UTILIZAÇÃO 8

3.1 REQUISITOS PARA A EMPRESA (OU ENTIDADE) 8

3.2 REQUISITOS PARA SOFTWARE DE FATURAÇÃO 8

4 FLUXOS 9

4.1 FLUXOS DE GESTÃO DE CONTA 9

4.1.1 Criação de conta de assinatura 9

4.1.1.1 Identificador de conta de assinatura 9

4.1.1.2 Autenticação do Cidadão 9

4.1.1.3 Elegibilidade do Cidadão 10

4.1.1.4 Fluxo de Criação de conta 10

4.1.1.5 AccessTokens 13

4.1.1.6 RefreshTokens 13

4.1.1.7 Data de validade da conta de assinatura 13

4.1.1.8 Data de validade do certificado 13

4.1.1.9 Estrutura da resposta de informação de conta de assinatura 14

4.1.1.10 Emissão de certificados e ativação de conta de assinatura 15

4.1.2 signatureAccount/updateToken 15

4.1.3 signatureAccount/cancel 16

4.2 FLUXOS DE ASSINATURA 17

4.2.1 info 17

4.2.2 credentials/list 17

4.2.3 credentials/info 18

4.2.4 /v2/credentials/authorize 18

4.2.5 /credentials/authorize/verify 18

4.2.6 /v2/signatures/signHash 19

4.2.7 /signatures/signHash/verify 19

4.3 EXEMPLO DE FLUXO TÍPICO 20

5 ESPECIFICAÇÃO DE SERVIÇOS 23

5.1 AMBIENTES 23

6 GERAÇÃO DE HASHES 24

7 IDENTIFICADOR ÚNICO DO CIDADÃO 25

7.1 TIPOS DE DOCUMENTOS ACEITES 25

7.2 EXEMPLOS DE IDENTIFICADORES ÚNICOS DE CIDADÃOS 25

8 PROCESSO DE INTEGRAÇÃO 26

9 GUIDELINES DE INTEGRAÇÃO 27

1 Introdução

O processamento de faturas em papel é um processo dispendioso para as empresas, com custos para cidadãos e empresas consumindo recursos à economia. De modo a melhorar e tornar mais seguro este processo, as entidades e empresas procuram proceder à desmaterialização das faturas.

A fatura eletrónica, uma fatura emitida e recebida em formato eletrónico, vem então dar resposta a esta necessidade de desmaterialização.

O Serviço de Assinatura de Faturas Eletrónicas (**SAFE**), enquadrado no Sistema de Certificação de Atributos Profissionais (SCAP), surge com o objetivo de suportar este processo de desmaterialização, estando conforme com o artigo 12º do DL 28/2019 de 15 de fevereiro.

Este serviço permite ao cidadão, enquanto profissional de uma empresa, assinar digitalmente faturas eletrónicas, através de mecanismo automatizado pelo software de faturação. No que respeita à garantia de autenticidade da origem desta fatura, assim como à garantia de integridade da mesma, será utilizado o procedimento de aposição de assinatura eletrónica qualificada do SAFE, em que a chave privada de assinatura (do colaborador da empresa com poderes para emitir e assinar faturas) é guardada centralmente de forma segura. O detentor da chave privada de assinatura terá que autorizar a utilização da mesma pelo software de faturação, sempre que a mesma é emitida ou renovada.

Este documento detalha os fluxos e especifica os serviços do SAFE. Para além disso, aborda também outros temas importantes como o processo de integração.

1.1 Definições, Acrónimos e Abreviações

SAFE – Serviço de Assinatura de Faturas Eletrónicas

SCAP – Sistema de Certificação de Atributos Profissionais

FA – Fornecedor de Autenticação

AMA – Agência para a Modernização Administrativa

CC – Cartão de Cidadão

CMD – Chave Móvel Digital

2 Arquitetura da Solução

O Serviço de Assinatura de Faturas Eletrónicas (**SAFE**) está inserido no ecossistema *Autenticacao.Gov* (ver Figura 1), tirando proveito das funcionalidades de sistemas já existentes. Nomeadamente:

- Fornecedor de Autenticação (**FA**) – responsável pela autenticação de cidadãos, podendo os cidadãos utilizar a Chave Móvel Digital (CMD) ou o Cartão de Cidadão (CC) para proceder à sua autenticação. Após correta autenticação, o FA comunica com o SAFE para criação de conta de assinatura de faturas eletrónicas;
- Sistema de Certificação de Atributos Profissionais (**SCAP**) – responsável pela gestão e obtenção de atributos, em particular, os empresariais de cidadãos. O SAFE comunica com o SCAP para verificar se um cidadão tem o atributo necessário para criar uma conta de assinatura de faturas eletrónicas.

O SAFE integra com estes dois sistemas no fluxo de criação de conta (ver 4.1.1). Este fluxo é iniciado pelo Software de Faturação, comunicando com o FA.

No que diz respeito aos fluxos de assinatura, são também iniciados pelo Software de Faturação, comunicando diretamente com o SAFE (ver 4.2).

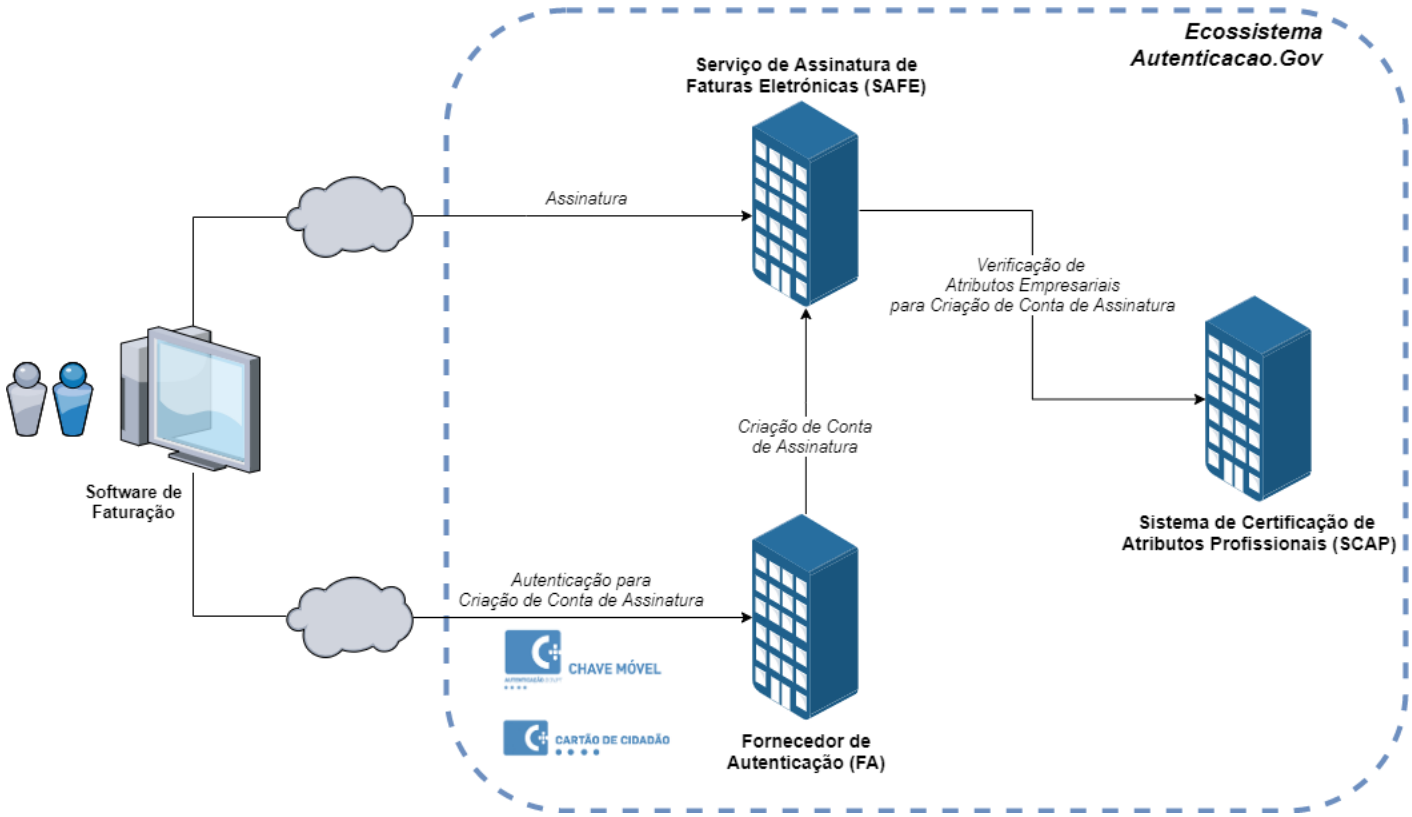

Figura 1. Ecossistema Autenticacao.Gov

3 Requisitos para utilização

3.1 Requisitos para a Empresa (ou Entidade)

- Acesso à Internet;
- Colaborador da empresa com poderes para emitir e assinar faturas, detém
    - Chave Móvel Digital + PIN de autenticação *ou* Cartão de Cidadão + PIN de autenticação + Leitor de Cartões;
    - Atributo "*Assinatura de faturas eletrónicas*" ativo no SCAP na empresa para a qual pretende criar conta de assinatura de faturas (ver mais informação em SAFE – Guias de Fluxos Complementares).

3.2 Requisitos para Software de Faturação

- Efetuar integração com SAFE e FA;
- Passar pelo Processo de Integração e credenciação (ver secção 8).

4 Fluxos

Esta secção descreve os fluxos necessários para que Softwares de Faturação possam integrar com o SAFE.

4.1 Fluxos de gestão de conta

4.1.1 Criação de conta de assinatura

A criação de uma conta de assinatura no SAFE é feita via Fornecedor de Autenticação (FA) que, após a devida autenticação do cidadão (colaborador da empresa com poderes para emitir e assinar faturas), encaminha o pedido de criação de conta de assinatura para o SAFE. Assim, neste fluxo, o Software de Faturação comunica apenas com o cidadão e com o FA.

4.1.1.1 *Identificador de conta de assinatura*

As contas de assinatura do SAFE são identificadas univocamente pelas seguintes componentes:

- Identificador único do cidadão (ver secção 7);
- NIPC da empresa;
- Informação adicional (campo opcional utilizado para o cidadão fazer distinção entre contas associadas à mesma empresa).

Deste modo, um cidadão pode ter múltiplas contas de assinatura, seja para a mesma empresa ou para empresas diferentes.

4.1.1.2 *Autenticação do Cidadão*

O cidadão autentica-se perante o FA, recorrendo a um dos seguintes meios:

- Chave Móvel Digital (CMD);
- Cartão de Cidadão (CC).

Mais informação sobre autenticações com CMD e CC pode ser encontrada em https://www.autenticacao.gov.pt/chave-movel-digital/autenticacao e https://www.autenticacao.gov.pt/cartao-cidadao/autenticacao, respetivamente.
Em ambiente de pré-produção, deverá ser utilizado o portal https://pprwww.autenticacao.gov.pt.

4.1.1.3 *Elegibilidade do Cidadão*

A validação da elegibilidade de um cidadão para criação de uma conta de assinatura como representante de uma empresa é feita pelo Sistema de Certificação de Atributos Profissionais (SCAP), através da existência do atributo ativo "*Assinatura de faturas eletrónicas*".
Para ativar e consultar os atributos do SCAP, o cidadão deverá autenticar-se em https://www.autenticacao.gov.pt/ e aceder à página https://www.autenticacao.gov.pt/area-privada/atributos-profissionais. Mais informação sobre os atributos do SCAP pode ser encontrada em https://www.autenticacao.gov.pt/a-autenticacao-de-profissionais.
Em ambiente de pré-produção, deverá ser utilizado o portal https://pprwww.autenticacao.gov.pt.

4.1.1.4 *Fluxo de Criação de conta*

O diagrama da Figura 2 ilustra o processo de criação de conta de assinatura no SAFE. Mais informações sobre integração com o FA podem ser encontradas em "*Autenticação.Gov - Manual de Integração*".
São em seguida descritos os passos deste fluxo:

1. Cidadão pede adesão ao serviço de assinatura de faturas, introduzindo os seguintes dados:
    a. NIPC da empresa associada à conta – **obrigatório (9 dígitos)**;
    b. Informação adicional da empresa – **opcional (máximo 100 caracteres).** Este campo tem como objetivo possibilitar que um cidadão possa criar várias contas de assinatura para a mesma empresa (e.g. local, departamento…);
    c. Email associado à conta – **obrigatório**;
    d. Data de validade da conta de assinatura – **opcional (formato AAAA-MM-DD)**;
    e. Número máximo de assinaturas – **obrigatório (máximo de 450000)**;
2. Software de Faturação invoca FA para o cidadão se poder autenticar. Esta autenticação será feita através do protocolo OAuth2 (ver mais informação em "*Autenticação.Gov - Manual de Integração"* e "*Guia rápido de utilização do OAuth2 do FA*"), e devem ser pedidos os seguintes atributos:
    a. http://interop.gov.pt/MDC/Cidadao/NIC *(se cidadão português)*
    b. http://interop.gov.pt/MDC/Cidadao/DocType[1] *(se cidadão estrangeiro)*
    c. http://interop.gov.pt/MDC/Cidadao/DocNationality[1] *(se cidadão estrangeiro)*
    d. http://interop.gov.pt/MDC/Cidadao/DocNumber[1] *(se cidadão estrangeiro)*
    e. http://interop.gov.pt/MDC/Cidadao/NomeProprio

[1] Ver formato na secção 7.

f. http://interop.gov.pt/MDC/Cidadao/NomeApelido
g. http://interop.gov.pt/MDC/Cidadao/DataValidade
h. http://interop.gov.pt/MDC/Cidadao/DataNascimento
i. http://interop.gov.pt/SAFE/createSignatureAccount?enterpriseNipc=<enterpriseNipc>$enterpriseAdditionalInfo=<enterpriseAdditionalInfo>$email=<email>$expirationDate=<expirationDate>$signaturesLimit=<signaturesLimit>$creationClientName=<creationClientName *(os valores entre <> devem ser substituídos pela informação introduzida no passo 1). No caso de alguma destas informações conter espaços em branco, os parâmetros do atributo (tudo o que vem depois do '?'), deve ser convertido numa string base64.*

3. FA mostra a página de autenticação no mecanismo utilizado pelo Software de Faturação (*e.g. WebView ou Browser*);
4. Cidadão efetua autenticação com CMD ou CC;
5. Página da autenticação envia dados para o FA;
6. FA valida a autenticação;
7. FA pede criação de conta de assinatura, enviando para o SAFE os dados obtidos na autenticação;
8. FA devolve um token OAuth associado à autenticação efetuada;
9. Software de Faturação verifica token OAuth associado à autenticação efetuada;
10. Software de Faturação obtém token OAuth associado à autenticação efetuada;
11. SAFE pede ao SCAP os atributos empresariais do cidadão na empresa para a qual pretende criar conta de assinatura;
12. SCAP devolve atributos empresariais do cidadão na empresa para a qual pretende criar conta de assinatura;
13. SAFE valida se o cidadão tem o atributo "*Assinatura de faturas eletrónicas*" na empresa para a qual pretende criar conta de assinatura;
14. SAFE cria conta de assinatura;
15. Software de Faturação invoca FA com o token OAuth obtido no passo 10, de forma a obter a informação de conta de assinatura. Antes de fazer esta invocação, o Software de Faturação deve esperar **15 segundos**;
16. FA valida token OAuth recebido;
17. FA pede informação de conta de assinatura;
18. SAFE devolve informação de conta de assinatura para o FA (ver mais informação no ponto 4.1.1.9);
19. FA devolve informação de conta de assinatura para o Software de Faturação (ver mais informação no ponto 4.1.1.9);
20. Software de Faturação guarda informação de conta de assinatura;
21. Software de Faturação mostra mensagem de sucesso ao cidadão.

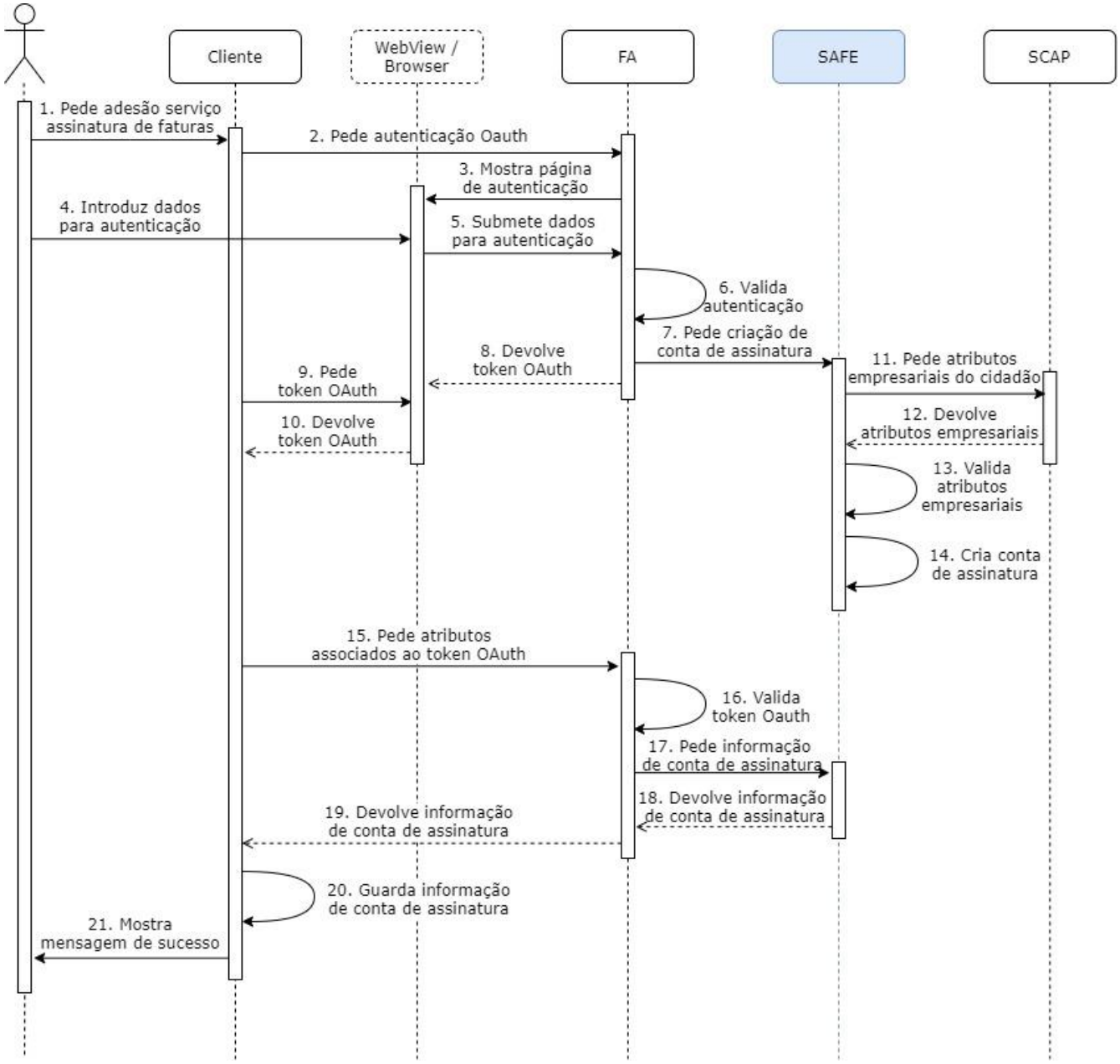

Figura 2. Fluxo de criação de conta de assinatura

4.1.1.5 *AccessTokens*

Token necessário para efetuar operações de assinatura no SAFE. Este token é do tipo Bearer e deve ser passado num custom header dos pedidos, chamado *SAFEAuthorization*.

Por uma questão de segurança, o *AccessToken* tem uma validade reduzida, definida pelo SAFE. Sempre que for invocado um método do SAFE com um *AccessToken* expirado, o SAFE retorna um erro HTTP **400 Bad Request**, com a mensagem de erro "*The access or refresh token is expired or has been revoked*". Nestes casos, o Software de Faturação deve invocar o método *signatureAccount/updateToken* (ver ponto 4.1.1.10), de modo a ser gerado um novo accessToken e um novo refreshToken. Estes novos tokens devem ser utilizados nas invocações futuras ao serviço.

4.1.1.6 *RefreshTokens*

Token necessário para invocar o método *signatureAccount/updateToken* (ver ponto 4.1.1.10). Este token é do tipo Bearer e deve ser passado num custom header dos pedidos, chamado *SAFEAuthorization*. O resultado da invocação do método *signatureAccount/updateToken* é a geração de um novo *accessToken* e de um novo *refreshToken*. Estes novos tokens devem ser utilizados nas invocações futuras ao serviço.

4.1.1.7 *Data de validade da conta de assinatura*

A data de validade de uma conta de assinatura é o menor dos seguintes valores:

- data de validade introduzida pelo cidadão no passo 1 do fluxo de criação de conta;
- data de validade do atributo "*Assinatura de faturas eletrónicas*" na empresa para a qual pretende criar conta de assinatura;
- data de validade máxima de uma conta no SAFE (45 dias).

4.1.1.8 *Data de validade do certificado*

A data de validade do certificado emitido é a data de validade do atributo "*Assinatura de faturas eletrónicas*" na empresa para a qual pretende criar conta de assinatura, acrescido de 30 dias.

4.1.1.9 *Estrutura da resposta de informação de conta de assinatura*

O FA devolve a informação de conta de assinatura para o Software de Faturação. Esta informação é enviada em formato json como valor do atributo http://interop.gov.pt/SAFE/createSignatureAccount.
Em caso de sucesso na criação de conta, são enviados os atributos:

- Token de acesso às operações de assinatura (*accessToken*);
- Token para atualização de tokens (*refreshToken*);
- Data de validade da conta de assinatura (*accountExpirationDate*);

Em caso de erro na criação de conta, são enviados os atributos:

- Erro (*error);*
- Descrição do erro (*error_description*);

As causas possíveis para se obter um erro, são (*error – error_description*):

- *Bad Request - Invalid parameter citizenDocId*
- *Bad Request - Missing parameter citizenDocId*
- *Bad Request - Invalid parameter citizenDocType*
- *Bad Request - Missing parameter citizenDocType*
- *Bad Request - Invalid parameter citizenDocCountry*
- *Bad Request - Missing parameter citizenDocCountry*
- *Bad Request - Invalid parameter enterpriseNipc*
- *Bad Request - Missing parameter enterpriseNipc*
- *Bad Request - Invalid parameter citizenDocId*
- *Bad Request - Missing parameter citizenDocId*
- *Bad Request - Invalid parameter enterpriseAdditionalInfo*
- *Bad Request - Missing parameter citizenGivenName*
- *Bad Request - Missing parameter citizenLastName*
- *Bad Request - Invalid parameter email*
- *Bad Request - Invalid parameter expidationDate, date must be in the future*
- *Bad Request - Invalid parameter signaturesLimit, should be higher or equal then 1*
- *Bad Request - Numbers of signatures is too high*
- *Bad Request - Missing parameter creationClientName*
- *Bad Request - Client is not active*
- *Missing required enterprise attributes - The citizen attributes obtained are not valid*
- *Internal Server Error - error_description: Unexpected error while processing client request*

4.1.1.10 *Emissão de certificados e ativação de conta de assinatura*

Depois do FA devolver uma resposta de sucesso com os tokens e data de validade de uma conta de assinatura (ver 4.1.1.9), a emissão dos certificados associados a essa conta prossegue de forma assíncrona, levando alguns segundos a ser concluída. Enquanto o certificado não for emitido, as invocações aos métodos do SAFE devolverão um erro HTTP **401 Unauthorized**. A emissão de certificados pode demorar até 120 segundos, pelo que o Software de Faturação deve assegurar um mecanismo de polling ao serviço durante esse tempo. Depois do certificado ter sido emitido, a conta passa ao estado ativo e os métodos do SAFE já poderão ser invocados com sucesso.

4.1.2 signatureAccount/updateToken

Método que retorna um novo *AccessToken* e um novo *RefreshToken* para uma conta de assinatura. Estes novos tokens devem ser utilizados nas invocações futuras aos serviços.

Este método deve ser invocado sempre que o sistema retorne o erro HTTP **400 Bad Request**, com a mensagem de erro "*The access or refresh token is expired or has been revoked*". A Figura 3 ilustra o processo de atualização de tokens. A especificação do método é apresentada na secção 5.

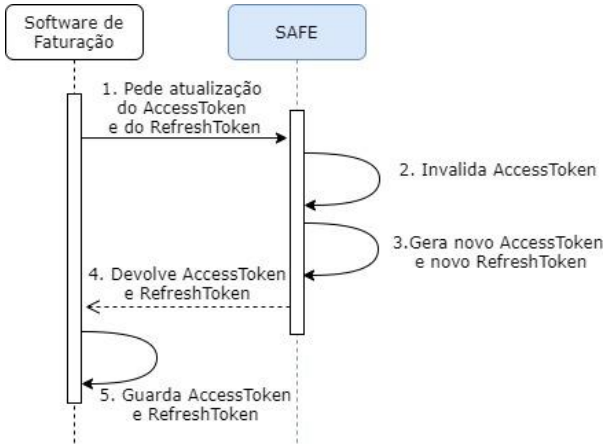

Figura 3. Fluxo de atualização de tokens

4.1.3 signatureAccount/cancel

Método que permite o cancelamento de uma conta de assinatura. A Figura 4 ilustra o processo cancelamento de uma conta de assinatura. A especificação do método é apresentada na secção 5.

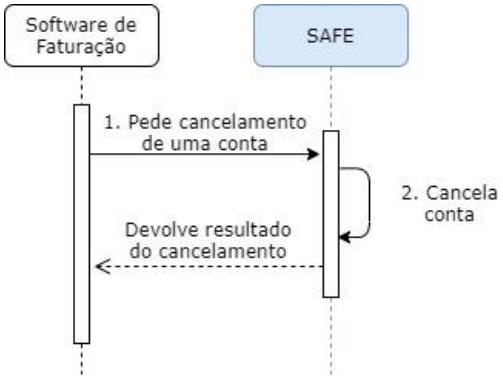

Figura 4. Fluxo de cancelamento de conta

4.2 Fluxos de Assinatura

O fluxo de assinatura segue o standard definido pelo *Cloud Signature Consortium* para assinatura remota (cf. Ref3).

4.2.1 info

Método que retorna informação sobre o serviço e a lista de todos os métodos implementados.

A Figura 5 ilustra o pedido de informação. A especificação do método é apresentada na secção 5.

Figura 5. Fluxo de pedido de informação

4.2.2 credentials/list

Método que retorna a lista de credenciais associados a uma conta de assinatura. Cada conta de assinatura do SAFE tem apenas uma credencial, que deve ser enviada em todos os métodos que requeiram o parâmetro *credentialId*.

A Figura 6 ilustra o pedido de credenciais de uma conta de assinatura. A especificação do método é apresentada na secção 5.

Figura 6. Fluxo de pedido de credenciais de uma conta

4.2.3 credentials/info

Método que retorna a informação associada a uma conta de assinatura. Nomeadamente, informação sobre o estado da conta de assinatura e a cadeia de certificados associados à conta de assinatura. A cadeia de certificados deve ser utilizada para construir os documentos assinados associadas à conta de assinatura. A Figura 7 ilustra o pedido de informação de uma conta de assinatura. A especificação do método é apresentada na secção 5.

Figura 7. Fluxo de pedido de informação de uma conta de assinatura

4.2.4 /v2/credentials/authorize

Método que pede autorização para efetuar uma assinatura. Neste método, o Software de Faturação deve gerar a(s) hash(es) do(s) documento(s) a assinar (ver mais informações sobre a geração da hash na secção 6), o SAFE regista a(s) hash(es) a assinar e gera um *Signature Activation Data* (SAD) que terá de ser enviado pelo Software de Faturação no pedido de assinatura (ver 4.2.6). Um SAD é único para cada pedido assinatura.

A primeira parte da Figura 8 (*/v2/credentials/authorize*) ilustra o pedido de autorização para efetuar uma assinatura. A especificação do método é apresentada na secção 5.

4.2.5 /credentials/authorize/verify

Método que verifica autorização para efetuar uma assinatura. Neste método, o Software de Faturação deve enviar o *processId* utilizado na invocação do método de pedido de autorização (ver 4.2.4). O SAFE devolve o Signature Activation Data (SAD) que terá de ser enviado pelo Software de Faturação no pedido de assinatura (ver 4.2.6). Um SAD é único para cada pedido assinatura. Este método deve ser invocado do seguinte modo: a primeira invocação deve ser feita 1 segundo após a invocação do

método de pedido de autorização (ver 4.2.4). Se o SAFE devolver um código HTTP **204 No Content** (ou seja, não devolver o SAD), o pedido deve ser repetido mais 4 vezes (total de 5 vezes), com intervalos de 1 segundo.

A segunda parte da Figura 8 (*/credentials/authorize/verify*) ilustra o pedido de verificação de uma autorização para efetuar uma assinatura. A especificação do método é apresentada na secção 5.

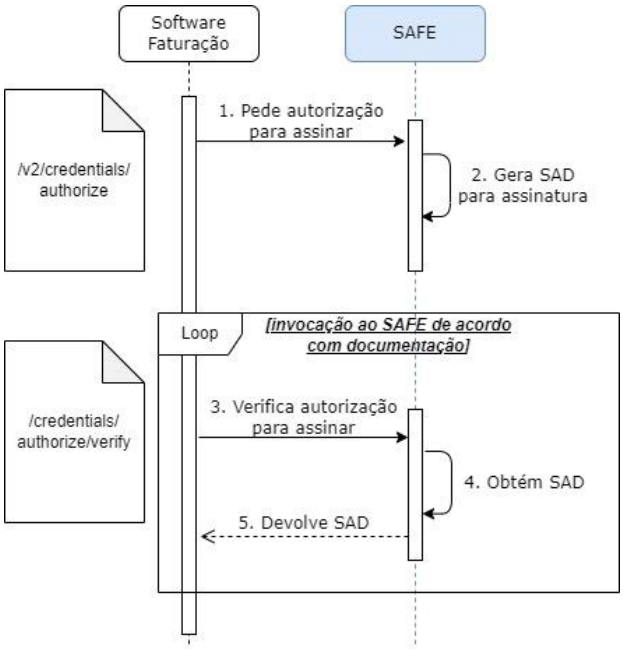

Figura 8. Fluxo de pedido de autorização para efetuar assinatura

4.2.6 /v2/signatures/signHash

Método que pede assinatura de hash(es). Este método que deve ser invocado após a invocação do método de verificação de autorização (ver 4.2.5), verifica se o SAD recebido corresponde ao que foi gerado no método de autorização, e assina a(s) hash(es) assinada(s).

A primeira parte da Figura 9 (*/v2/signatures/signHash*) ilustra o pedido de assinatura. A especificação do método é apresentada na secção 5.

4.2.7 /signatures/signHash/verify

Método que retorna a(s) hash(es) assinada(s). Este método deve ser invocado após a invocação do método de pedido de assinatura autorização (ver 4.2.6). O Software de Faturação deve enviar o

processId utilizado na invocação do método de pedido de assinatura (ver 4.2.6) e o SAFE verifica se a assinatura já foi efetuada. Se sim, o SAFE devolve a(s) hash(es) assinada(s). Neste passo, o Software de Faturação deve construir o documento assinado, juntando, ao documento original, a hash assinada do documento e os certificados obtidos no método *credentials/info* (ver 4.2.3). Este método deve ser invocado do seguinte modo: a primeira invocação deve ser feita 1 segundo após a invocação do método de pedido de assinatura (ver 4.2.6). Se o SAFE devolver um código HTTP **204 No Content** (ou seja, não devolver a(s) hash(es) assinada(s)) o pedido deve ser repetido mais 4 vezes (num total de 5 vezes), com intervalos de 1 segundo.

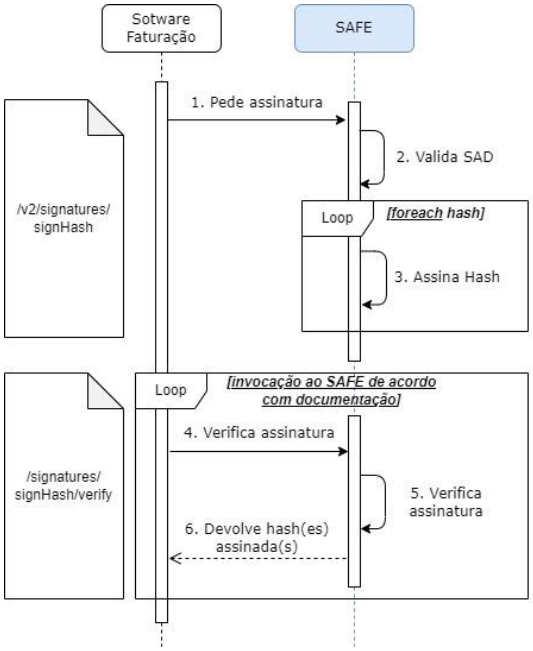

Figura 9. Pedido de assinatura

4.3 Exemplo de Fluxo Típico

A Figura 10, pretende ilustrar um exemplo de fluxo típico da comunicação entre o Software de Faturação e o FA e SAFE. O fluxo começa com o Software de Faturação a comunicar com o FA pedindo a criação de uma conta de assinatura.

Após correta criação de conta, o Software de Faturação passa a comunicar exclusivamente com o SAFE, enviando o *AccessToken* ou o *RefreshToken* obtidos na criação de conta. Estes tokens são do tipo Bearer e devem ser passados num custom header dos pedidos, chamado *SAFEAuthorization*. O *RefreshToken* é enviado no método de atualização de tokens (s*ignatureAccount/updateToken).* Para os restantes métodos, é enviado o *AccessToken*.

No método *credentials/list* é obtida a credencial da conta de assinatura. Esta credencial deve ser enviada como parâmetro nos métodos seguintes.

No método *credentials/info* é obtida informação sobre a conta de assinatura. Nomeadamente, informação sobre o estado da conta de assinatura e a cadeia de certificados associados à conta de assinatura. A cadeia de certificados devolvida neste método deve ser utilizada para construir o documento assinado.

Sempre que o cidadão pretenda efetuar uma assinatura, deve ser invocado o método v2/*credentials/authorize*. Neste método deve(m) ser enviada(s) a(s) hash(es) do(s) documento(s) a assinar (ver mais informações sobre a geração da hash na secção 6). Para além disso, tem também de ser enviado, na mesma ordem, o(s) nome(s) do(s) documento(s) a assinar. O método devolve apenas um código HTTP **200 OK** em caso de sucesso. Depois disso, deve ser invocado o método */credentials/authorize/verify* passando o *processId* utilizado na invocação anterior, de modo a obter um *Signature Activation Data* (SAD) que terá de ser enviado no pedido de assinatura.

No método *v2/signatures/signHash* é(são) novamente enviada(s) a(s) hash(es) do(s) documento(s) a assinar assim como o SAD devolvido no passo anterior. O método devolve apenas um código HTTP **200 OK** em caso de sucesso. Depois disso, deve ser invocado o método */signatures/signHash/verify* passando o *processId* utilizado na invocação anterior, de modo a obter a(s) hash(es) assinada(s). Neste passo, o Software de Faturação deve construir o documento assinado, juntando, ao documento original, a hash assinada do documento e os certificados obtidos no método *credentials/info*. Na construção do(s) documento(s) assinado(s) é recomendado que o Software de Faturação utilize *Long-Term Validation* (LTV).

No caso de o *AccessToken* se encontrar expirado, o SAFE devolve um erro HTTP **400 Bad Request**, com a mensagem de erro "*The access or refresh token is expired or has been revoked*". Nestes casos, o Software de Faturação deve invocar o método *SignatureAccount/updateToken* (ver ponto 4.1.1.10), de modo a ser gerado um novo accessToken e um novo refreshToken. Estes novos tokens devem ser utilizados nas invocações futuras ao SAFE.

No caso em que o cidadão pretenda cancelar a conta de assinatura, deve ser invocado o método *signatureAccount/cancel*.

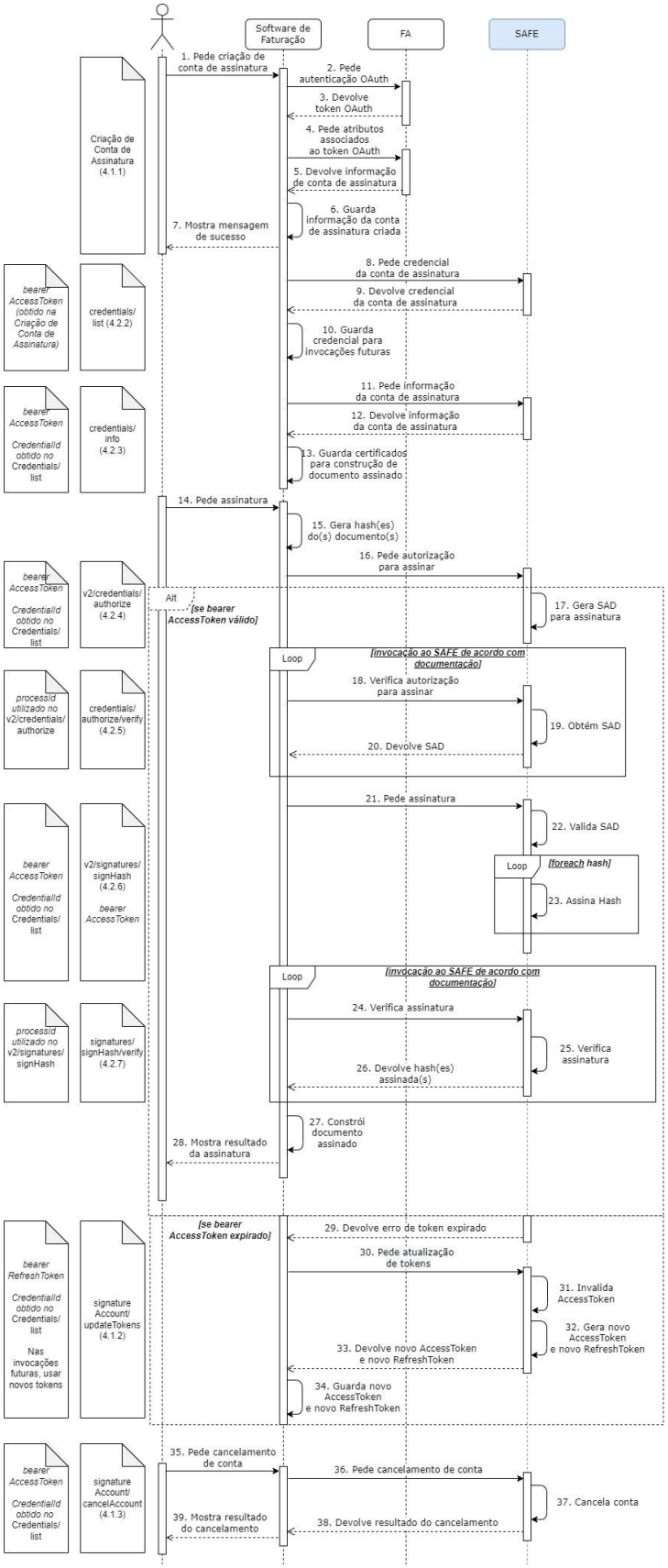

Figura 10. Fluxo típico

5 Especificação de Serviços

Em anexo a este documento, são partilhados também os ficheiros que contêm as especificações dos serviços do SAFE. Estes documentos estão formatados segundo a especificação da OpenAPI (https://swagger.io/specification) e podem ser lidos por qualquer ferramenta de leitura de especificações OpenAPI (e.g. https://editor.swagger.io).

Os métodos definidos, seguem a especificação definida no documento "*Architectures and protocols for remote signature applications*" do Cloud Signature Consortium.

A comunicação entre o Software de Faturação e o SAFE deve ser feita através do protocolo HTTPS com basic authentication.

As credenciais de basic authentication, assim como o valor do campo *clientName* e do *clientId* para autenticação OAuth serão facultadas aos Softwares de Faturação, aquando da sua integração com o SAFE e com o FA. Todos os métodos expostos pelo SAFE têm um parâmetro *processId*, que espera um novo *Globally Unique Identifier* (GUID) para cada invocação.

Em ambiente de pré-produção, podem ser utilizadas, numa fase inicial, as seguintes credenciais:

- basic authentication - *user: clientTest; password: Test*
- clientName – *clientTest*

5.1 Ambientes

Os métodos que constam na especificação estão publicados nos ambientes que constam da Tabela 1.

Ambiente	Domínio
Pré-Produção	https://pprsafe.autenticacao.gov.pt
Produção	https://safe.autenticacao.gov.pt

Tabela 1. Ambientes

6 Geração de hashes

A geração da hash deve ser feita segundo os passos 1 e 2 do ponto 9.2 da especificação "*PKCS #1: RSA Cryptography Specifications Version 2.2*" (disponível em https://tools.ietf.org/html/rfc8017#page-45).

Ou seja, após ser gerada a hash (com o algoritmo SHA-256) de um documento, deve ser adicionado o prefixo correspondente ao algoritmo SHA-256:

```
byte[] sha256SigPrefix =
    { 0x30, 0x31, 0x30, 0x0d, 0x06, 0x09, 0x60, (byte) 0x86, 0x48, 0x01, 0x65,
    0x03, 0x04, 0x02, 0x01, 0x05, 0x00, 0x04, 0x20 };
```

A hash enviada para assinatura deve ser a concatenação do *sha256SigPrefix* com a hash do documento.

7 Identificador Único do Cidadão

O identificador único do cidadão segue a norma *ETSI 319 412-1* para cidadãos estrangeiros. Para cidadãos portugueses, são utilizados os carateres "BI" em vez de "IDC". Esta norma identifica o cidadão através dos seguintes elementos:

1. Tipo do documento;
2. País do documento;
3. Identificação do documento.

7.1 Tipos de documentos aceites

Os tipos de documentos aceites pelo SAFE são:

1. **BI** – Cartão de Cidadão / Bilhete de Identidade
2. **PAS** – Passaporte
3. **TR:** – Título de Residência
4. **CR:** – Cartão de Residência

7.2 Exemplos de Identificadores Únicos de cidadãos

Exemplo para cidadão português

1. Tipo do documento – **BI**
2. País do documento – **PT**
3. Identificação do documento – **12345678**

Exemplo para cidadão estrangeiro com passaporte

1. Tipo do documento – **PAS**
2. País do documento – **BR**
3. Identificação do documento – **12345678**

Exemplo para cidadão estrangeiro com título de residência (TR:) / cartão de residência (CR:)

1. Tipo do documento – **TR:**
2. País do documento – **BR**
3. Identificação do documento – **12345678**

8 Processo de Integração

De modo a poder integrar com o SAFE, a entidade responsável por um Software de Faturação tem de:

1. Enviar email para eid@ama.pt a formalizar a intenção de integrar com o SAFE;
2. Celebrar protocolo com a AMA;
3. Produzir relatório assinado com evidências de cumprimento de *Guidelines de Integração* (ver 9);
4. Realizar processo de certificação da solução, enviando:
    - Vídeo demonstrativo da solução;
    - 5 exemplares de documentos assinados;
    - Código fonte da aplicação para certificação por parte da AMA. Como alternativa, pode também ser pedida a certificação da aplicação a uma entidade externa independente e credenciada para auditorias eIDAS.
5. Receber credenciais de *Basic Authentication* e *ClientName* para integração com o SAFE;
6. Receber *ClientId* para integração OAuth.

9 Guidelines de Integração

O Software de Faturação deve cumprir as guidelines que constam de ficheiro em anexo.