Agency for Administrative Modernization IP

# Electronic Invoice Signing Service

## Integration Document

Version 2.0

AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA

## References to other Documents

| Ref. | Description | Author |
|---|---|---|
| Ref1 | Authentication.Gov - Integration Manual | LOVE |
| Ref2 | FA OAuth2 Quick Start Guide | LOVE |
| Ref3 | Architectures and protocols for remote signature applications – Published version 1.0.4.0 (2019-06) | Cloud Signature Consortium |
| Ref4 | SAFE - Complementary Flow Guides | LOVE |

## Revision Record

| Date | Version | Description | Author |
|---|---|---|---|
| 03-09-2020 | 0.9 | Initial Document | Tiago Brás |
| 2020-09-11 | 1.0 | Revised Initial Document | André Vasconcelos |
| 2020-10-06 | 1.1 | Reviewing account creation data | Tiago Brás |
| 2020-10-21 | 1.2 | Reviewing account creation data | Tiago Brás |
| 11-18-2020 | 1.3 | Addition of reference to flows complementary and possible responses for account creation, alteration of authorization headers | Tiago Brás |
| 2021-02-22 | 1.4 | Changing SCAP attribute name and clarification | Tiago Brás |
| 2021-03-01 | 1.5 | Fix expiration error code tokens and clarification | Tiago Brás |
| 03-03-2022 | 1.6 | Change of integration process and clarification | Tiago Brás |
| 2022-10-24 | 2.0 | Updating subscription services | Tiago Brás |

# Index

# 1. Introduction

Processing paper invoices is a costly process for businesses, with costs for citizens and businesses consuming resources to the economy. In order to improve and make this safer process, entities and companies seek to dematerialize invoices.

The electronic invoice, an invoice issued and received in electronic format, thus responds to this need for dematerialization.

The Electronic Invoice Signature Service **(SAFE),** within the Professional Attributes Certification System (SCAP), arises with the aim of supporting this dematerialization process, in accordance with article 12 of DL 28/2019 of 15 February.

This service allows the citizen, as a company professional, to digitally sign electronic invoices, through an automated mechanism by the invoicing software. With regard to guaranteeing the authenticity of the origin of this invoice, as well as guaranteeing its integrity, the SAFE qualified electronic signature procedure will be used, in which the private signature key (of the company employee with powers to issue and sign invoices) is centrally stored securely. The holder of the private signature key will have to authorize its use by the invoicing software, whenever it is issued or renewed.

This document details the flows and specifies the SAFE services. Furthermore, it also addresses other important topics such as the integration process.

## *1.1 Definitions, Acronyms and Abbreviations*

**SAFE** – Electronic Invoice Signature Service

**SCAP** - Professional Attributes Certification System

**FA** - Authentication Provider

**AMA** – Agency for Administrative Modernization

**CC** - Citizen Card

**CMD** - Digital Mobile Key

# 2 Solution Architecture

The Electronic Invoice Signature Service **(SAFE)** is part of the *Autenticacao.Gov* ecosystem (see Figure 1), taking advantage of the functionality of existing systems. Namely:

- Authentication Provider **(FA)** – responsible for the authentication of citizens, being able to citizens to use the Mobile Digital Key (CMD) or the Citizen Card (CC) to proceed your authentication. After correct authentication, the FA communicates with SAFE to create electronic billing account;
- Professional Attributes Certification System **(SCAP)** – responsible for the management and obtaining attributes, in particular, the entrepreneurial ones of citizens. SAFE communicates with SCAP to verify that a citizen has the necessary attribute to create a signing electronic invoices.

SAFE integrates with these two systems in the account creation flow (see 4.1.1). This flow starts by the Billing Software, communicating with the FA.

With regard to subscription flows, they are also initiated by the Billing Software, communicating directly with SAFE (see 4.2).

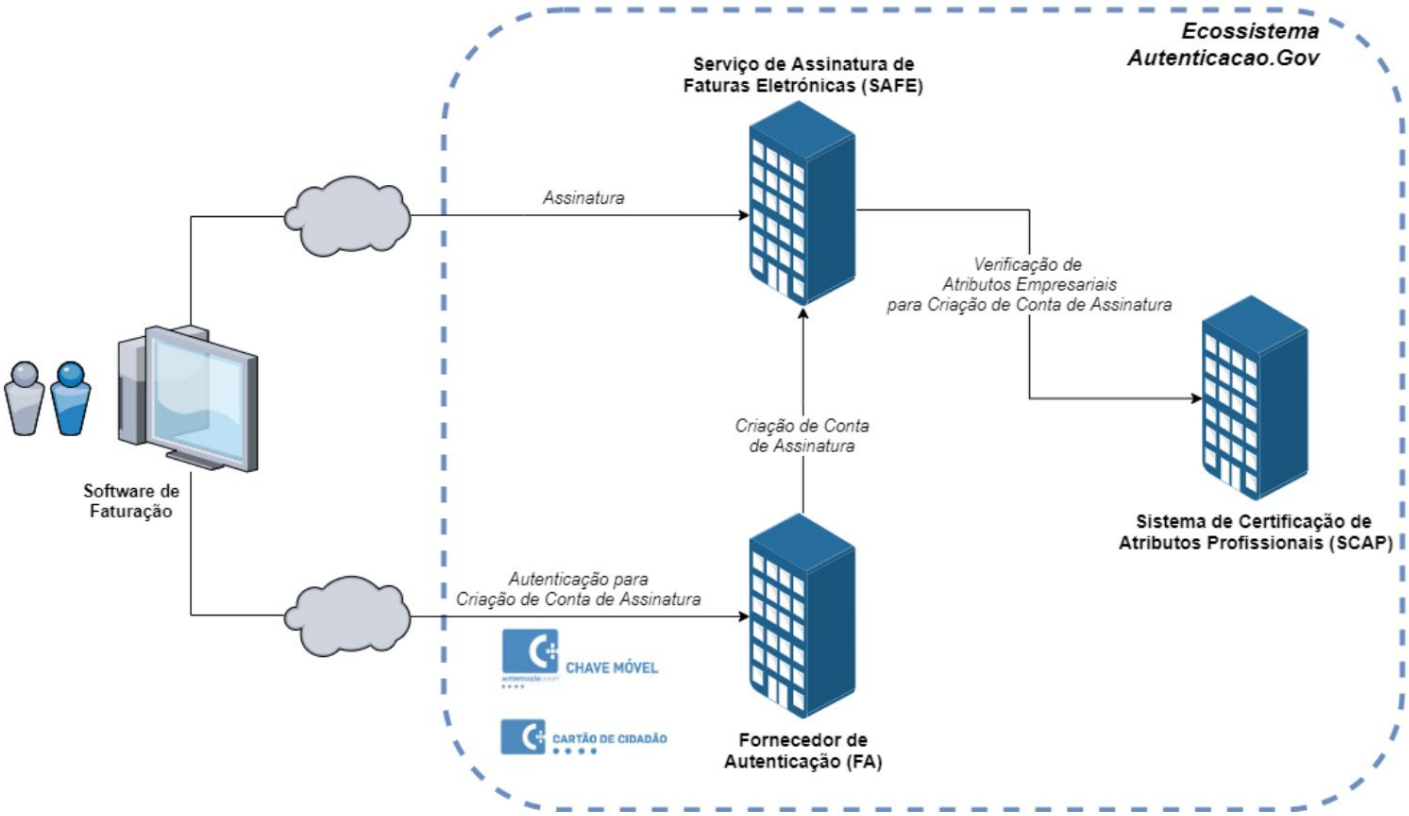


Figure 1. Autenticacao.Gov Ecosystem

# 3 Requirements for use

## *3.1 Requirements for the Company (or Entity)*

- Internet access;
- Company employee with powers to issue and sign invoices, holds
  - o Digital Mobile Key + authentication PIN *or* Citizen Card + authentication + Card Reader;
  - o Attribute *"Electronic invoice signature"* active in SCAP in the company for which want to create an invoice subscription account (see more information in SAFE – Complementary Flow Guides).

## *3.2 Requirements for Billing Software*

- Integrate with SAFE and FA;
- Go through the Integration and Accreditation Process (section 8).

# 4 Flows

This section describes the flows necessary for Invoicing Software to integrate with the SAFE

## *4.1 Account Management Flows*

### 4.1.1 Creating a Subscription Account

The creation of a subscription account in SAFE is done via the Authentication Provider (FA) that, after the due authentication of the citizen (company employee with powers to issue and sign invoices), forwards the subscription account creation request to SAFE. Thus, in this flow, the Invoicing Software communicates only with the citizen and with the FA.

#### 4.1.1.1 *Subscription Account Identifier*

SAFE subscription accounts are uniquely identified by the following components:

- Unique citizen identifier (see section 7);
- Company NIPC;
- Additional information (optional field used for the citizen to distinguish between accounts associated with the same company).

In this way, a citizen can have multiple subscription accounts, either for the same company or for different companies.

#### 4.1.1.2 *Citizen Authentication*

The citizen authenticates himself before the FA, using one of the following means:

- Digital Mobile Key (CMD);
- Citizen Card (CC).

More information on authentications with CMD and CC can be found at https://www.authenticacao.gov.pt/chave-movel-digital/authenticacao and

In a pre-production environment, the portal https://pprwww.autenticacao.gov.pt should be used.

#### 4.1.1.3 *Citizen Eligibility*

Validation of the eligibility of a citizen to create a subscription account as a representative of a company is carried out by the Professional Attributes Certification System (SCAP), through the existence of the active attribute *"Signature of electronic invoices".*

To activate and consult the SCAP attributes, the citizen must authenticate himself at https://www.authenticacao.gov.pt/ and access the page https://www.authenticacao.gov.pt/area privata/atributos-profissionais . More information about SCAP attributes can be found at https://www.authenticacao.gov.pt/a-authenticacao-de-profissionais.

In a pre-production environment, the portal https://pprwww.authenticacao.gov.pt should be used.

#### 4.1.1.4 *Account Creation Flow*

The diagram in Figure 2 illustrates the subscription account creation process in SAFE. More information about FA integration can be found in *"Autenticação.Gov - Integration Manual".*

The steps of this flow are described below:

1. Citizen requests subscription to the invoice signing service, introducing the following data:
   - The. NIPC of the company associated with the account – **mandatory (9 digits);**
   - B. Additional company information – **optional (maximum 100 characters).** This field is intended to enable a citizen to create multiple accounts subscription for the same company (eg location, department…);
   - ç. Email associated with the account – **required;**
   - d. Subscription account expiration date – **optional (YYYY-MM-DD format);**
   - and. Maximum number of subscriptions – **mandatory (maximum 450000);**
2. Invoicing Software invokes FA so that the citizen can authenticate himself. This authentication will be done through the OAuth2 protocol (see more information in *"Autenticação.Gov - Integration Manual"* and " FA *OAuth2 Quick Start Guide* "), and must be requests the following attributes:
   - *The.* http://interop.gov.pt/MDC/Cidadao/NIC *(if Portuguese citizen)*
   - *B.* http://interop.gov.pt/MDC/Cidadao/DocType 1 *(if foreign citizen)*
   - ç. http://interop.gov.pt/MDC/Cidadao/DocNationality1 *(if foreign citizen)*
   - *d.* http://interop.gov.pt/MDC/Cidadao/DocNumber1 *(if foreign citizen)*
   - and. http://interop.gov.pt/MDC/Cidadao/NomeProprio

[1] See format in section 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=<enterprise Nipc>$enterpriseAdditionalInfo=<enterpriseAdditionalInfo>$email=<email>$expi rationDate=<expirationDate>$signaturesLimit=<signaturesLimit>$creationClient Name=<creationClientName *(values between <> must be replaced by the information entered in step 1). In case any of this information contains blanks, the attribute parameters (everything that comes after the '?'), must be converted to a base64 string.*

3. FA shows the authentication page in the mechanism used by the Billing Software *(eg WebView or Browser);*
4. Citizen authenticates with CMD or CC;
5. Authentication page sends data to FA;
6. FA validates authentication;
7. FA requests the creation of a subscription account, sending to SAFE the data obtained in the authentication;
8. FA returns an OAuth token associated with the authentication performed;
9. Billing Software verifies OAuth token associated with authentication performed;
10. Billing Software obtains OAuth token associated with the authentication performed;
11. SAFE asks SCAP for the corporate attributes of the citizen in the company for which it intends create subscription account;
12. SCAP returns corporate attributes of the citizen in the company for which it intends to create subscription account;
13. SAFE validates if the citizen has the attribute *"Signature of electronic invoices"* in the company for which you want to create a subscription account;
14. SAFE creates subscription account;
15. Billing Software invokes FA with the OAuth token obtained in step 10, in order to obtain the subscription account information. Before making this invocation, the Software Billing must wait **15 seconds;**
16. FA validates received OAuth token;
17. FA asks for subscription account information;
18. SAFE returns subscription account information to the FA (see more information in point 4.1.1.9);
19. FA returns subscription account information to the Billing Software (see more information in point 4.1.1.9);
20. Billing Software saves subscription account information;
21. Invoicing software shows success message to citizen.

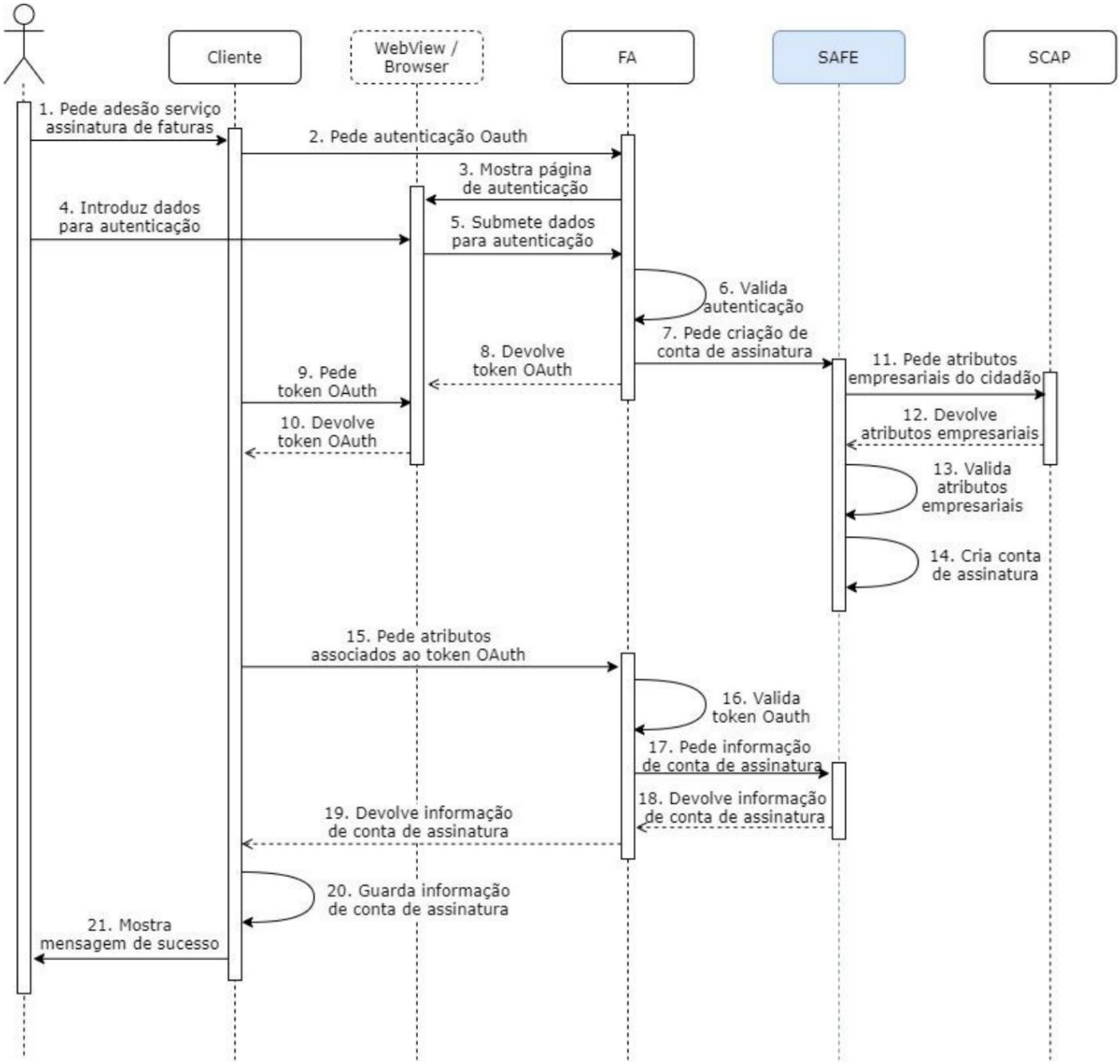


**Figure 2. Subscription account creation flow**

#### 4.1.1.5 *AccessTokens*

Token required to perform signature operations on SAFE. This token is of the Bearer type and must be passed in a custom header of requests, called *SAFEAuthorization.*

For security reasons, the *AccessToken* has a reduced validity, defined by SAFE. Whenever a SAFE method is invoked with an expired *AccessToken ,* SAFE returns an HTTP **400 Bad Request error,** with the error message *"The access or refresh token is expired or has been revoked".* In these cases, the Billing Software must invoke the method *signatureAccount/ updateToken* (see point 4.1.1.10), in order to generate a new accessToken and a new refreshToken. These new tokens must be used in future service invocations.

#### 4.1.1.6 *RefreshTokens*

Token required to invoke the *signatureAccount/ updateToken* method (see point 4.1.1.10). This token is of type Bearer and must be passed in a custom header of requests, called *SAFEAuthorization.* The result of invoking the *signatureAccount/ updateToken* method is the generation of a new *accessToken* and a new *refreshToken.* These new tokens must be used in future service invocations.

#### 4.1.1.7 *Subscription account expiration date*

The expiration date of a subscription account is the lesser of the following values:

- expiration date entered by the citizen in step 1 of the account creation flow;
- expiry date of the attribute *"Electronic invoice signature"* in the company for which want to create subscription account;
- maximum expiration date of a SAFE account (45 days).

#### 4.1.1.8 *Certificate validity date*

The expiry date of the certificate issued is the expiry date of the attribute *"Signature of electronic invoices"* in the company for which you want to create a subscription account, plus 30 days.

#### 4.1.1.9 *Structure of Subscription Account Information Response*

The FA returns the subscription account information to the Billing Software. This information is sent in json format as the value of the http://interop.gov.pt/SAFE/createSignatureAccount attribute .
In case of successful account creation, the attributes are sent:

- Access token for subscription operations *(accessToken);*
- Token for refreshing tokens *(refreshToken);* • Subscription account expiration date *(accountExpirationDate);*

In case of an error when creating an account, the attributes are sent:

- Error *(error);*
- Error description *(error_description);*

Possible causes for getting an error are *(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 expirationDate, date must be in the future • Bad Request - Invalid parameter signaturesLimit, should be higher or equal then 1 • Bad Request - Numbers of signatures it's 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 *Issuing certificates and activating subscription account*

After the FA returns a successful response with the tokens and expiry date of an account signature (see 4.1.1.9), the issuance of certificates associated with that account proceeds in a asynchronous, taking a few seconds to complete. As long as the certificate is not issued, invocations to SAFE methods will return an HTTP **401 Unauthorized error.** after the certificate has been issued, the account becomes active and the SAFE methods can now be invoked with success.

### 4.1.2 signatureAccount/updateToken

Method that returns a new *AccessToken* and a new *RefreshToken* for a subscription account. These new tokens must be used in future service invocations.

This method must be invoked whenever the system returns the HTTP **400 Bad Request error,** with the error message *"The access or refresh token is expired or has been revoked".* Figure 3 illustrates the token refresh process. The method specification is presented in section 5.


**Figure 3. Token refresh flow**

### 4.1.3 signatureAccount/cancel

Method that allows the cancellation of a subscription account. Figure 4 illustrates the process canceling a subscription account. The method specification is presented in section 5.


**Figure 4. Account cancellation flow**

### *4.2 Subscription Flows*

The signature flow follows the standard defined by the *Cloud Signature Consortium* for remote signing (cf. Ref3).

#### 4.2.1 info

Method that returns information about the service and a list of all implemented methods.

Figure 5 illustrates the information request. The method specification is presented in section 5.


**Figure 5. Information request flow**

#### 4.2.2 credentials/list

Method that returns the list of credentials associated with a subscription account. Each SAFE subscription account has only one credential, which must be submitted in all methods that require the *credentialId* parameter .

Figure 6 illustrates the request for credentials from a subscription account. The method specification is presented in section 5.


**Figure 6. Account credential request flow**

### 4.2.3 credentials/info

Method that returns information associated with a subscription account. In particular, information about the state of the subscribing account and the certificate chain associated with the subscribing account. THE certificate chain must be used to build the signed documents associated with the signing account. Figure 7 illustrates requesting information from a subscription account. The method specification is presented in section 5.


**Figure 7. Flow of requesting information from a subscription account**

### 4.2.4 /v2/credentials/authorize

Method that asks for authorization to make a subscription. In this method, the Invoicing Software must generate the hash(es) of the document(s) to be signed (see more information about the hash generation in section 6), SAFE records the hash(es) to be signed and generates a *Signature Activation Data* (SAD) that will have to be sent by the Billing Software in the subscription order (see 4.2.6). A SAD is unique to each subscription order.

The first part of Figure 8 *(/v2/credentials/authorize)* illustrates the authorization request to perform a signature. The method specification is presented in section 5.

### 4.2.5 /credentials/authorize/verify

Method that checks authorization to make a subscription. In this method, the Billing Software must send the *processId* used in invoking the authorization request method (see 4.2.4).OSAFE returns the Signature Activation Data (SAD) that must be sent by the Billing Software in the signature request (see 4.2.6). A SAD is unique to each subscription order. This method must be invoked as follows: the first invocation must be done 1 second after the invocation of the

authorization request method (see 4.2.4). If SAFE returns an HTTP **204 No Content code ( ie** does not return the SAD), the request must be repeated 4 more times (total of 5 times), at 1 second intervals.

The second part of Figure 8 *(/ credentials/ authorize/ verify)* illustrates the request to verify a authorization to make a subscription. The method specification is presented in section 5.

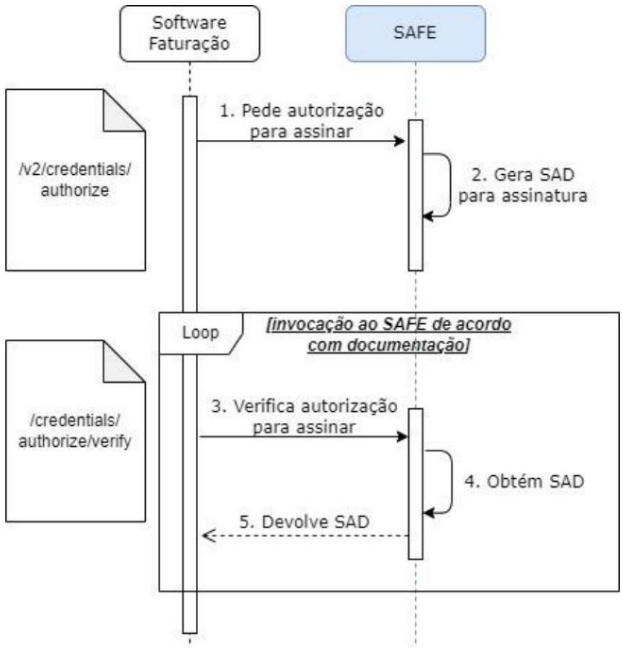


**Figure 8. Flow of authorization request to perform signature**

### 4.2.6 /v2/signatures/signHash

Method that asks for hash(es) signature. This method that must be invoked after invoking the authorization verification method (see 4.2.5), verifies that the received SAD matches what was generated in the authorization method, and signs the signed hash(es).

The first part of Figure 9 *(/ v2/ signatures/ signHash)* illustrates the signature request. The method specification is presented in section 5.

### 4.2.7 /signatures/signHash/verify

Method that returns the signed hash(es). This method must be invoked after invoking the authorization signature request method (see 4.2.6). The Billing Software must send the

*processId* used in invoking the signature request method (see 4.2.6) and SAFE checks if the signature has already been done. If so, SAFE returns the signed hash(es). In this step, the Invoicing Software must build the signed document, adding the signed hash of the document and the certificates obtained in the *credentials/ info* method to the original document (see 4.2.3). This method must be invoked as follows: the first invocation must be made 1 second after the invocation of the subscription request method (see 4.2.6). If SAFE returns an HTTP **204 No Content** (or i.e. not returning the signed hash(es) the request must be repeated 4 more times (a total of 5 times), with 1 second intervals.

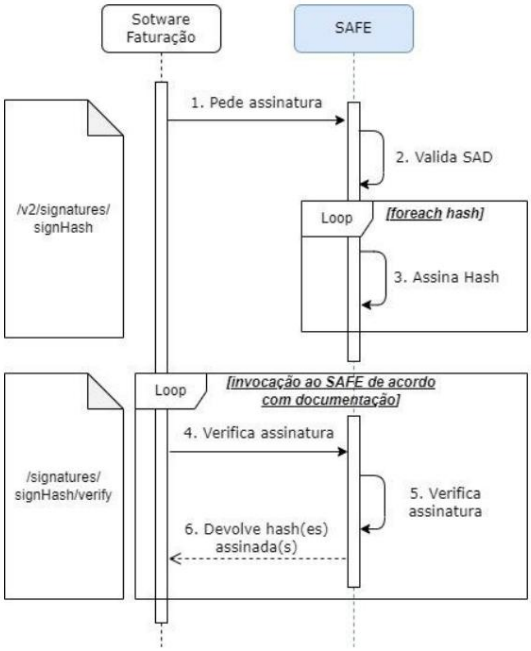


**Figure 9. Subscription request**

## *4.3 Typical Flow Example*

Figure 10, intends to illustrate an example of a typical flow of communication between the Invoicing Software and the FA and SAFE. The flow starts with the Billing Software communicating with the FA asking to create a subscription account.

After correct account creation, the Billing Software starts to communicate exclusively with SAFE, sending the *AccessToken* or *RefreshToken* obtained at account creation. These tokens are of the type Bearer and must be passed in a custom header of the requests, called *SAFEAuthorization.* The *RefreshToken* is sent in the token update method *(signatureAccount/ updateToken).* For the remaining methods, the *AccessToken is sent.*

In the *credentials/ list* method, the credential of the subscription account is obtained. This credential must be sent as a parameter in the following methods.

In the *credentials/ info* method, information about the subscription account is obtained. Namely, information about the subscription account status and the certificate chain associated with the subscription account. signature. The certificate chain returned in this method must be used to build the signed document.

Whenever the citizen wants to make a signature, the *v2/ credentials/ authorize method must be invoked.* In this method, the hash(es) of the document(s) to be signed must be sent (see more information on generating the hash in section 6). In addition, there is also be sent, in the same order, the name(s) of the document(s) to be signed. The method only returns an HTTP **200 OK** code on success. After that, the method must be invoked */ credentials/ authorize/ verify* passing the *processId* used in the previous invocation, in order to obtain a *Signature Activation Data* (SAD) that must be sent in the signature request.

In the *v2/ signatures/ signHash* method, the hash(es) of the document(s) to sign as well as the SAD returned in the previous step. The method only returns an HTTP **200** code **OK** on success. After that, the */signatures/ signHash/ verify* method must be invoked passing the *processId* used in the previous invocation, in order to obtain the signed hash(es). In this step, the Invoicing Software must build the signed document, adding, to the original document, the signed hash of the document and the certificates obtained in the *credentials/ info method.* When building the signed document(s), it is recommended that the Invoicing Software use *Long Term Validation* (LTV).

In case the *AccessToken* is expired, SAFE returns an HTTP **400 Bad Request error,** with the error message *"The access or refresh token is expired or has been revoked".* In these cases, the Billing Software must invoke the *SignatureAccount/ updateToken* method (see point 4.1.1.10), in order to generate a new accessToken and a new refreshToken. These new tokens must be used in future invocations to SAFE.

In case the citizen wants to cancel the subscription account, the *signatureAccount/ cancel* method must be invoked .

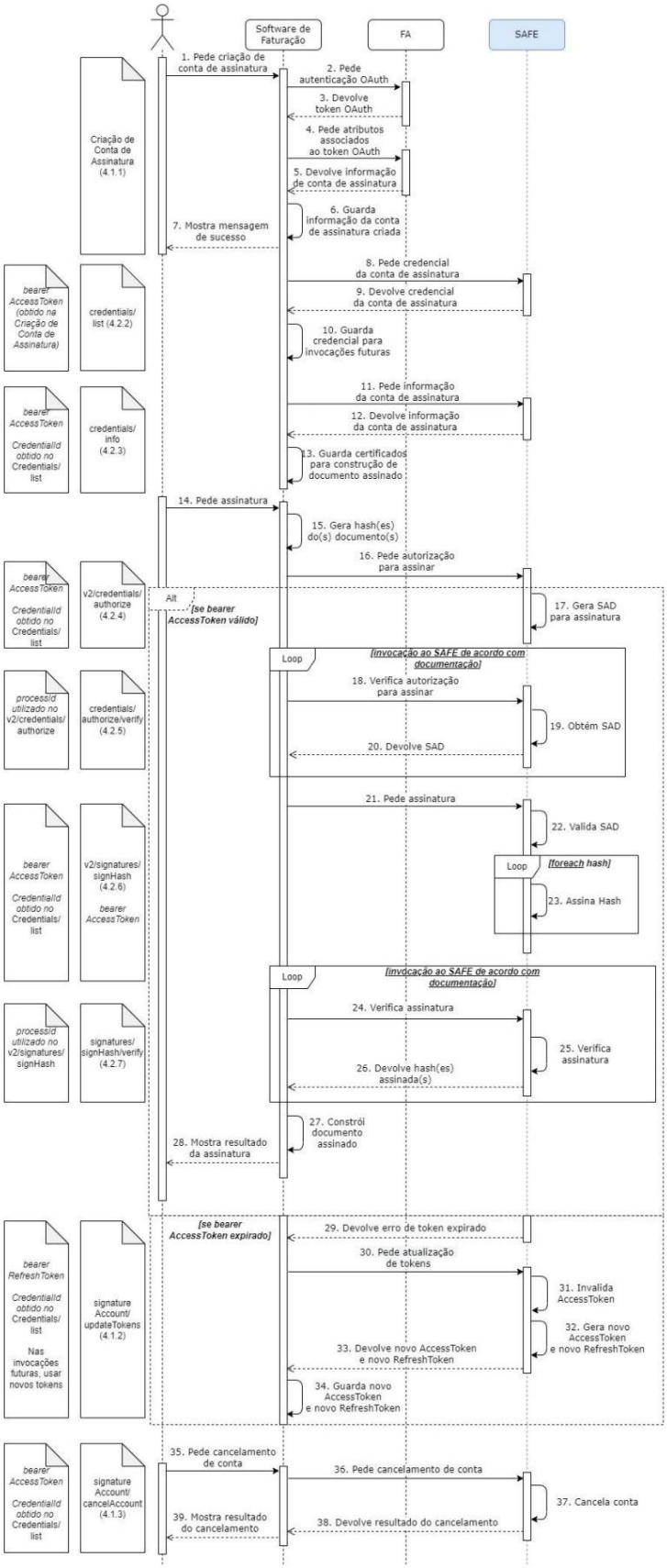


**Figure 10. Typical flow**

# 5 Service Specification

Attached to this document, files containing specifications for SAFE services are also shared. These documents are formatted according to the OpenAPI specification (https://swagger.io/specification) and can be read by any OpenAPI specifications (eg https://editor.swagger.io).

The defined methods follow the specification defined in the Cloud Signature Consortium document *"Architectures and protocols for remote signature applications"* .

The communication between the Billing Software and the SAFE must be done through the HTTPS protocol with basic authentication.

The basic authentication credentials, as well as the value of the *clientName* field and the *clientId* for OAuth authentication will be provided to the Billing Software, when integrating with SAFEe and FA. All methods exposed by SAFE have a *processId parameter,* which expects a new *Globally Unique Identifier* (GUID) for each invocation.

In a pre-production environment, the following credentials can be used at an early stage:

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

## *5.1 Environments*

The methods included in the specification are published in the environments listed in Table 1.

| Environment | Domain |
|---|---|
| **Pre-Production** | https://pprsafe.authenticacao.gov.pt |
| **Production** | https://safe.authenticacao.gov.pt |

**Table 1. Environments**

# 6 Hash generation

The hash generation must be done according to steps 1 and 2 of point 9.2 of the *"PKCS #1: RSA Cryptography Specifications Version 2.2" specification* (available at https://tools.ietf.org/html/rfc8017#page-45) .

That is, after the hash is generated (with the SHA-256 algorithm) of a document, the prefix corresponding to the SHA-256 algorithm:

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

The hash sent for signature must be the concatenation of *sha256SigPrefix* with the document hash.

# 7 Unique Citizen Identifier

The unique citizen identifier follows the *ETSI 319 412-1* standard for foreign nationals. For Portuguese citizens, the characters “BI” are used instead of “IDC”. This standard identifies the citizen through the following elements:

1. Document type;
2. Country of the document;
3. Document identification.

## *7.1 Types of documents accepted*

The types of documents accepted by SAFE are:

1. **BI** – Citizen Card / Identity Card
2. **PAS** - Passport
3. **TR:** – Residence Title
4. **CR:** – Residence Card

## *7.2 Examples of Unique Citizen Identifiers*

**Example for Portuguese citizen**

1. Document Type - **BI**
2. Country of the document – **PT**
3. Document identification - **12345678**

**Example for foreign citizen with passport** 1. Type of document – **PAS**

2. Country of the document - **BR**
3. Document identification - **12345678**

**Example for foreign citizen with residence permit (TR:) / residence card (CR:)**

1. Type of document - **TR:**
2. Country of the document - **BR**
3. Document identification - **12345678**

# 8 Integration Process

In order to integrate with SAFE, the entity responsible for a Billing Software must:

1. Send an email to eid@ama.pt to formalize your intention to integrate with SAFE;
2. Sign a protocol with the AMA;
3. Produce a signed report with evidence of compliance with *Integration Guidelines* (see 9);
4. Carry out the solution certification process, sending:
   - o Video demo of the solution;
   - o 5 copies of signed documents;
   - o Application source code for AMA certification. Alternatively, you can certification of the application may also be requested from an independent and accredited external entity for eIDAS audits.
5. Receive *Basic Authentication* and *ClientName* credentials for SAFE integration;
6. Get *ClientId* for OAuth integration.

# 9 Integration Guidelines

The Billing Software must comply with the guidelines contained in the attached file.