|  |  |
| --- | --- |
| **BOSA signature solution**  FPS information | bosa.png |

# Summary

This document is intended for an FPS (Federal Public Service) that wishes to integrate the BOSA signature solution ‘Federal Trust Services’ (FTS). It allows users (Belgian citizens or residents) who are surfing on the FPS website to sign a document with their eID or foreigner card. This document, for example a PDF or XML, has been prepared or created by the FPS.  
  
The whole signing process is handled by BOSA. The FPS only has to upload the unsigned document to BOSA, redirect the user to BOSA and wait for a callback; then the signed document can be downloaded.

Contents

[1. Introduction FTS 2](#_Toc78283716)

[1.1. Singing flow 2](#_Toc78283717)

[2. Getting started 4](#_Toc78283718)

[2.1. Environments and development process 4](#_Toc78283719)

[2.2. Code repositories 4](#_Toc78283723)

[2.3. Main URLs 5](#_Toc78283726)

[2.4. IP adresses BOSA 6](#_Toc78283728)

[2.5. Signing profiles 6](#_Toc78283729)

[2.6. Example code 7](#_Toc78283730)

[3. Details 7](#_Toc78283731)

[3.1. BOSA S3 server 8](#_Toc78283732)

[3.2. The getToken call 8](#_Toc78283733)

[3.3. The HTTP redirect 9](#_Toc78283734)

[3.4. The callback to the FPS 9](#_Toc78283735)

[3.5. PDF visible signatures 12](#_Toc78283736)

[3.6. Disabling downloads 14](#_Toc78283737)

[3.7. Request a specific language when calling the service WEB UI 15](#_Toc78283738)

[3.8. Using XLST file 15](#_Toc78283739)

[3. Sample/test FPS code and service 15](#_Toc78283740)

[References 16](#_Toc78283741)

# Introduction FTS

The FTS uses 2 components to sign with eID: a web browser extension and a local component. Installing the software does not require admin rights. The signing procedure will take care of the installation if the components are missing. For organizations an msi installer is available for deployment. These are the supported environments:

* windows/mac/linux
* firefox/chrome (+edge)/safari/internet explorer

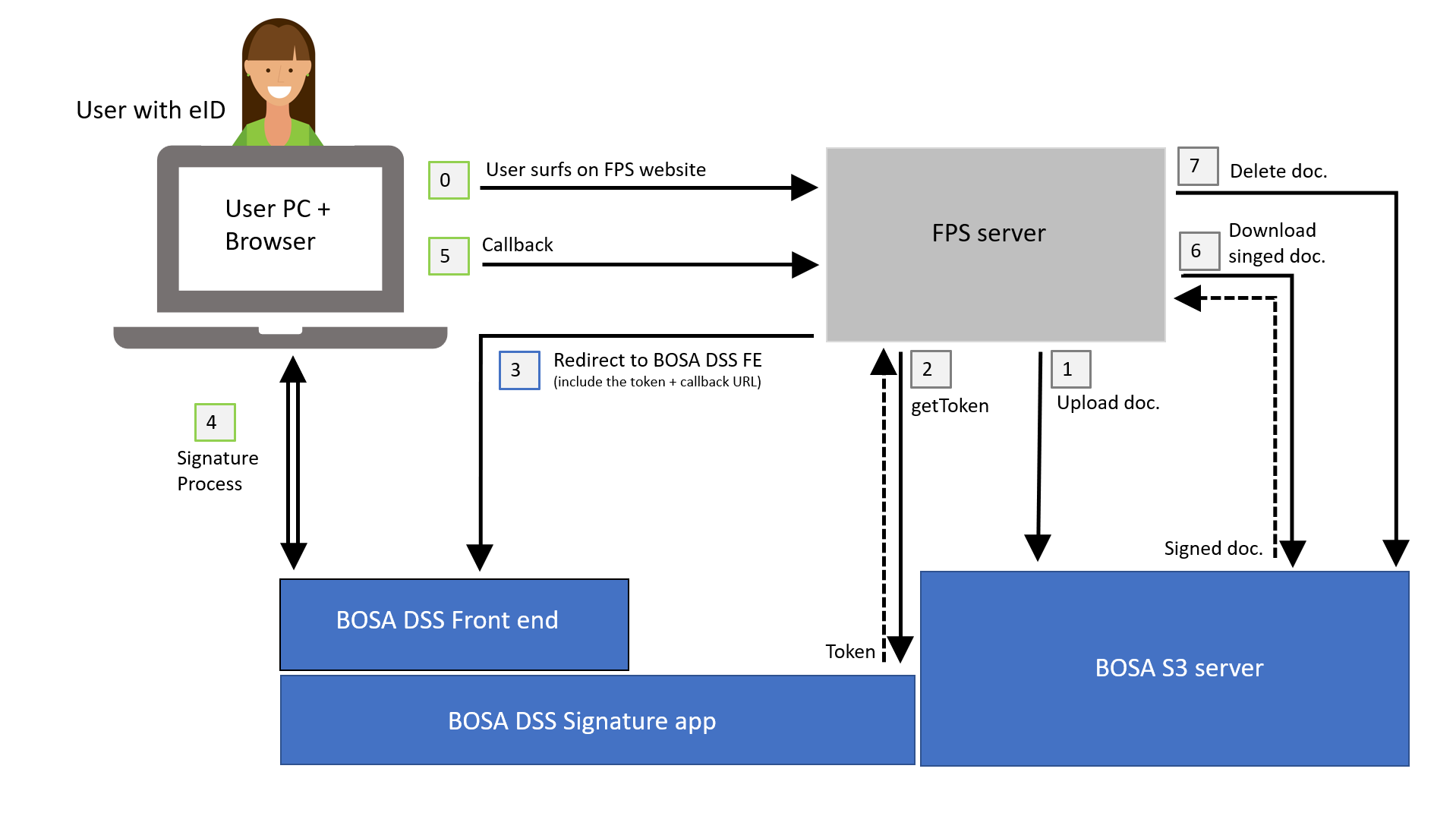
## **Singing** flow

The signing service FTS flow consists of 3 parties:

* An **FPS** that wants a User to sign a document with his/her eID/foreigner card
* A **User** (citizen, resident) with his/her PC, surfing on the FPS website
* **BOSA**, who offers the signing services

The flow goes as follows:

1. The User is surfing on the FPS website
2. The FPS creates a document (to be signed by the User) and uploads it to the BOSA S3 server  
   In case of an XML document, a corresponding XSLT file can optionally be uploaded too
3. The FPS sends a ‘getToken’ request to the BOSA DSS server and gets back a *token*
4. The FPS redirects the User to the BOSA DSS front-end server, this HTTP redirect includes the token and a *callback URL*
5. The actual signature process is done between the User and BOSA, at the end a signed document is put on the BOSA S2 server
6. A callback to the FPS is done
7. The FPS downloads the signed document
8. The FPS deletes the unsigned and signed documents



# 2. Getting started

## 2.1. Environments and development process

|  |  |  |
| --- | --- | --- |
| **TA** | TEST | continuously deployed from commits to “developer” code branch. |
| **QA** | QUALITY | continuously deployed from commits to “master” code branch. |
| **INT** | INTEGRATION | deployed from stable release. |
| **PROD** | PRODUCTION | deployed from stable release. IP filtering will be required. |

### Day-to-Day development

* On “developer” code branch
* Deployed automatically to TA
* New features
* Bug fixing

### Feature complete development

* On “master” code branch
* Deployed automatically to QA
* Development always starts in TA
* Stable releases: tagged versions for the service that can be rolled out to PROD and INT

### Deliverables and artifacts

* Open source development model
* Based on Docker containers
* BOSA service is based on the latest stable version hereof

## 2.2. Code repositories

### GitLab

* BOSA hosted and private
* Primary repository
* Main branches: “developer” and “master”
* Integrated with build & deploy pipeline for all environments
* Only TA and QA autodeploy when new code gets committed

### GitHub

* Public code repository
* Automated mirror from GitLab
* Exact copy of “master” branch
* Includes release tags so FTS PROD version can be checked out from the code
* Repositories
  + <https://github.com/Fedict/fts-test-environment>
    - script for local deployment of signing service for testing
  + <https://github.com/Fedict/fts-mintest>
    - code for mintest code example, a basic implementation how to call the service
  + <https://github.com/Fedict/fts-documentation>
    - Repository for documentation and architecture documents
  + <https://github.com/Fedict/fts-sign-validation>
    - Signing and validation engine
  + <https://github.com/Fedict/fts-gui-sign>
    - Signing frontend application (webflows)
  + <https://github.com/Fedict/fts-esealing>
    - Sealing application
  + <https://github.com/Fedict/fts-eidlink>
    - Client application (BeidConnect – repository to be renamed)

## 2.3. Main URLs

URLs are based on QA.

* Replace QA with TA or INT for those environments
* Remove QA in the URL for PROD

Example:

*PROD: https://dp.fts.bosa.belgium.be*

*TA: https://dp.ta.fts.bosa.belgium.be  
QA: https://dp.qa.fts.bosa.belgium.be  
INT: https://dp.int.fts.bosa.belgium.be*

### URLs

* [https://dp.qa.fts.bosa.belgium.be](https://dp.fts.bosa.belgium.be/)
  + URL for the storage bucket
  + API endpoint
  + WEBUI to manage the bucket (including password reset)
  + MINIO webUI available
* [https://sign.qa.fts.bosa.belgium.be](https://sign.fts.bosa.belgium.be/)
  + URL for the signing application
  + API endpoint
* [https://validate.qa.fts.bosa.belgium.be/signandvalidation/signing/getTokenForDocument](https://validate.fts.bosa.belgium.be/signandvalidation/signing/getTokenForDocument)
  + URL for Token request
  + API endpoint
* [https://sign.qa.fts.bosa.belgium.be/sign](https://sign.fts.bosa.belgium.be/sign) (yet to be launched)
  + WEBUI with manual procedure (upload and sign)
* [https://mintest.qa.fts.bosa.belgium.be](https://mintest.fts.bosa.belgium.be/)
  + Hosted version of fts-test-environment application
  + Implements full flow using the storage bucket and redirection
* [https://validate.qa.fts.bosa.belgium.be/signandvalidation/swagger-ui.html](https://validate.fts.bosa.belgium.be/signandvalidation/swagger-ui.html)
  + Swagger overview of REST API

## 2.4. IP adresses BOSA

IP addresses behind CallBackUrl.

|  |  |  |
| --- | --- | --- |
| **TA** | ECOSYS-NONPUB-TA | 193.191.245.151 |
| **QA** | ECOSYS-NONPUB-QA | 193.191.245.150 |
| **INT** | ECOSYS-NONPUB-QA | 193.191.245.150 |
| **PROD** | ECO-HIDE-PR-PUB | 193.191.245.204 |

## 2.5. Signing profiles

URL: <https://github.com/Fedict/fts-sign-validation/tree/master/parameters/signature>

These are profiles that are used to instruct the service what type of signature to generate.

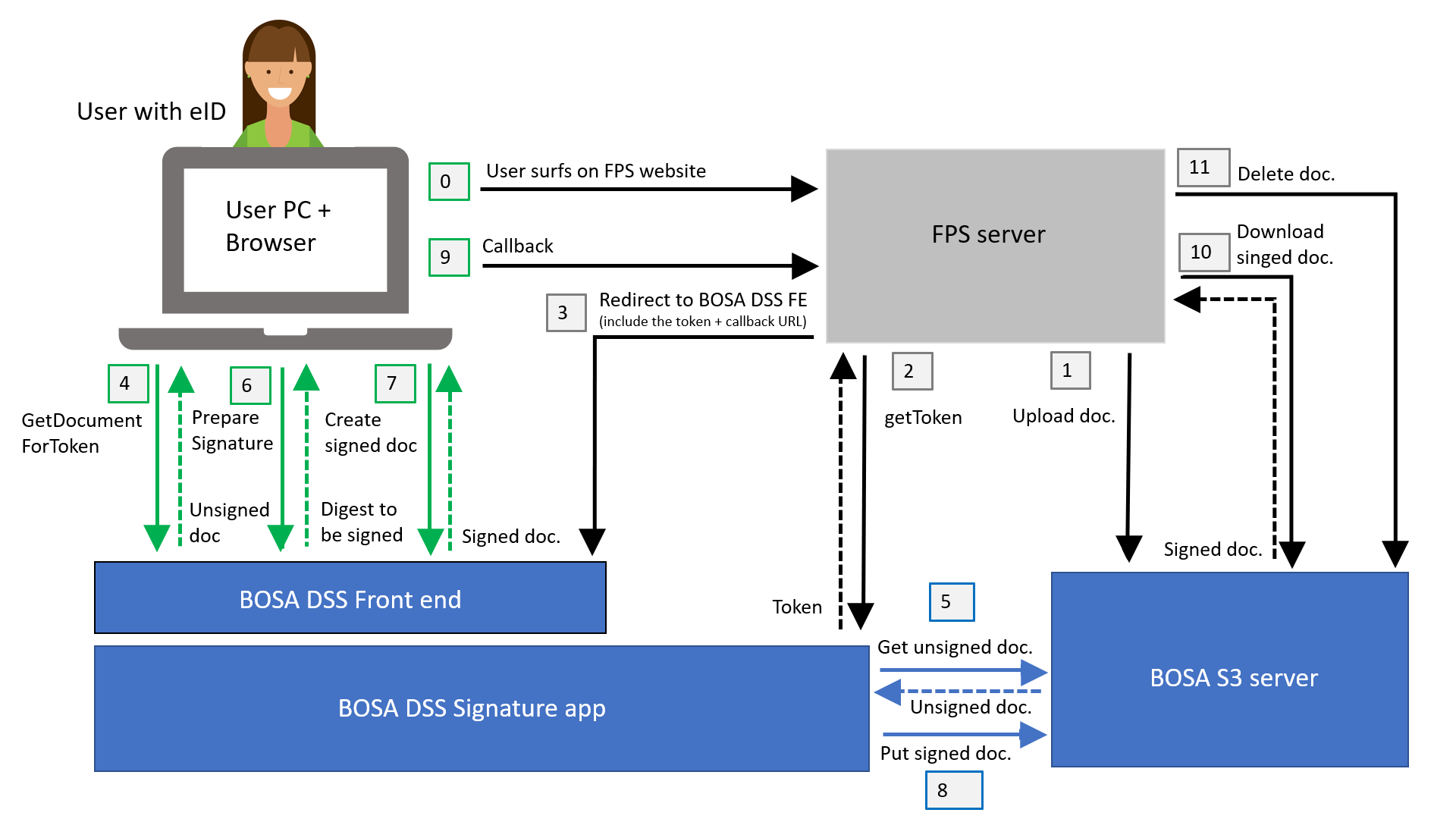
|  |  |  |  |
| --- | --- | --- | --- |
| **PROFIELNAAM** | **PROFIEL** | **FORMAAT** | **REMARK** |
| CADES\_1 | CAdES\_BASELINE\_B | ASiC\_S |  |
| CADES\_2 | CAdES\_BASELINE\_B | ASiC\_E |  |
| CADES\_LTA | CAdES\_BASELINE\_LTA | ASiC\_E DETACHED |  |
| CADES\_LTA\_ENVELOPING | CAdES\_BASELINE\_LTA | ENVELOPING |  |
| PADES\_1 | PAdES\_BASELINE\_B | ENVELOPED |  |
| PADES\_LTA | PAdES\_BASELINE\_LTA | ENVELOPED |  |
| PADES\_LTA\_EXP\_ALLOW | PAdES\_BASELINE\_LTA | ENVELOPED | **ALLOWS SIGNING WITH EXPIRED CERTIFICATES. NOT AVAILABLE IN INT/PROD** |
| XADES\_1 | XAdES\_BASELINE\_B | ENVELOPED |  |
| XADES\_2 | XAdES\_BASELINE\_B | ENVELOPING |  |
| XADES\_LTA | XAdES\_BASELINE\_LTA | ENVELOPED |  |
| XADES\_LTA\_EXP\_ALLOW | XAdES\_BASELINE\_LTA | ENVELOPED | **ALLOWS SIGNING WITH EXPIRED CERTIFICATES. NOT AVAILABLE IN INT/PROD** |

|  |
| --- |
| **B: SIGNATURE WITH CERTIFICATE CHAIN** |
| **T: B + TIME STAMP** |
| **LT: T + REVOCATION DATA** |
| **LTA: LT + 2ND TIME STAMP** |

## 2.6. Example code

* source on <https://github.com/Fedict/fts-test-environment/tree/master/mintest>
* hosted as-is on [https://mintest.qa.fts.bosa.belgium.be](https://mintest.qa.fts.bosa.belgium.be/)

# 3. Details



## **3.1. BOSA S3 server**

BOSA provides an Amazon S3 compatible server: MinIO [1].

The FPS uses this server to:

* Upload unsigned documents and additional files such as XSLT files or ‘PDF signature profiles’
* Download signed documents
* Delete the unsigned and signed documents

When the FPS registers for the signature solution, it receives a username and password for this BOSA S3 server. With this, the FPS can then upload, download and delete documents.

*It is important to note that this BOSA S3 server is not intended for long time storage: the space allocated to an FPS is limited, and the FPS itself is responsible for timely deleting documents that are no longer needed.*

There are free client SDKs available for several languages (Java, python, .NET, …) on [2].  
An FPS can use these to implement the upload/download/delete calls.

Implementation note: to connect to an S3 server, typically 3 things are needed: a ‘bucket name’ (this can be seen as a directory on the S3 server), a username and a password.  
For the BOSA S3 server however, the ‘bucket name’ and username are the same, therefore only a username and password are provided during the registration.

## 3.2. The getToken call

This is a REST call (a HTTP POST containing a json string) from the FPS to the BOSA DSS server; the BOSA DSS server will return a ‘token’.

This token is a string that contains a.o. the names of the unsigned (‘in’) and signed (‘out’) documents. It is cryptographically protected so they can’t be modified. Note: that it has nothing to do with OAuth or OpenID.

For the FPS, this token is transparent and does not have to be parsed/interpreted/.. It only has to be sent in the HTTP redirect call to the BOSA DSS front-end server.

Here is an example of the contents of a getToken request:

|  |
| --- |
| *{*  *"name":"minfin",*  *"pwd":"U84SnLEQvp",*  *"in":"test.xml",*  *"xslt":"test.xslt",*  *"out":"signed\_test.xml",*  *"prof":"XADES\_1"*  *}* |

The “xslt” parameter is optional. It can be used when the input document is an XML file and it use by the user’s browser to convert the XML file into HTML code for viewingin the browser.

The “prof” parameter specifies which type of signature is requested. BOSA provides a list of the available values and their meaning.

## 3.3. The HTTP redirect

After the FPS has uploaded the document and obtained the token, it will do a HTTP redirect of the User’s browser to the BOSA DSS front-end server; this will handle the actual signing process.

This redirect contains the following parameters:

* The token obtained in the getToken call: this is at the end of the URL path
* A callback URL to the FPS: this is a query parameter
* A language parameter: this is a query parameter. Values: en, nl, fr, de
* A name parameter: this is used to show the FPS name in the User’s browser

Example of a redirect URL:

|  |
| --- |
| *https://sign.ta.fts.bosa.belgium.be/sign/SDZEgF935d6e9.DKEi8D7nFDZz8EEZLazemJFeLIE.2FIDsdf987dILEJFd?callback=http%3A%2F%2F%2Feservices.minfin.fgov.be%2Fcallback%3Ffilename%3Dsigned\_test.pdf&language=en&name=FPS%20XXX* |

With the token, the user’s browser will download the unsigned document and, if present, the XSLT file from the BOSA DSS server. It will then display the document (the PDF, the XML or the XLST-transformed XML) and read out the certificates from the User’s eID/foreigner card. It will then ask to enter the PIN and proceed with the actual signing.

## 3.4. The callback to the FPS

After the document is signed and available on the BOSA S3 server, the User’s browser will do a callback to the callback URL specified in the redirect (see above). The callback URL is completely specified by the FPS and can contain query parameters like a session ID.

Next to the signed document, a json file is added to the BOSA S3 server that contains the signing certificate and the simple and the detailed validation report. The filename of this json file is the output filename of the signed document, appended with ".validationreport.json" (e.g. if the filename of the signed document = "*8uSOFNM03ns4F8N.xml*" then filename of the json file = "*8uSOFNM03ns4F8N.xml.validationreport.json*") Just like the other files, it is up to the FPS to delete this json file.

If the validation report will be used/saved by the FPS, it should be downloaded and then deleted from the S3 at the same time as the signed document. This is to avoid the case that a document with the same name should (accidentally) be used while the validation report of the previous signed document is still present. In case of doubt, it is possible to link both together by means of the reference-id as shown below:

|  |  |
| --- | --- |
| Signed document:signed_doc.png | *Validation report:*  validation_report.png |

In case of an error, the following parameters are added:

* err: an error string, e.g. *CERT\_REVOKED*
* details: a string with error details, this parameter is optional
* ref: a unique reference

Examples of a full callback URL:

|  |
| --- |
| ***http://eservices.minfin.fgov.be/callback?session=349317359*** |

|  |
| --- |
| ***http://eservices.minfin.fgov.be/callback?session=762087326****&ref=20210423092112378&err=CERT\_REVOKED* |

|  |
| --- |
| ***http://eservices.minfin.fgov.be/callback?session=650807315****&ref=20210423091821774&details=* *exp.%20date%20=%202017.05.29%2022:00:00&err=SIGN\_CERT\_EXPIRED* |

The bold part is the original callback URL specified by the FPS in the redirect, the rest has been added by the browser’s javascript.

Below is a list of the error strings that have been defined so far:

|  |  |
| --- | --- |
| **Error constant** | **Explanation** |
| BEID\_CONNECT\_ERROR | Couldn't connect to the eID card |
| NO\_READER | No reader found on the user's PC |
| UNSUPPORTED\_READER | unsupported smart card reader |
| SIGNATURE\_FAILED | eID card returned an invalid signature |
| CARD\_BLOCKED | eID card blocked |
| CARD\_ERROR | eID card error |
| USER\_CANCELLED | User cancelled the signing operation |
| SIGN\_CERT\_EXPIRED | Signing certificate expired |
| CERT\_CHAIN\_INCOMPLETE | No or incomplete certificate chain |
| NO\_SIGN\_CERT | No signing certificate provided |
| INVALID\_SIG\_DATE | Signing date out of bounds |
| INVALID\_S3\_LOGIN | Invalid user name or password |
| NO\_CERT\_TO\_VALIDATE | The certificate is missing |
| NO\_DOC\_TO\_VALIDATE | DSSDocument is null |
| NO\_TOKEN | Required parameter token not provided |
| CERT\_REVOKED | Certificate (probably the signing cert) revoked |
| INTERNAL\_ERR | Unexpected error occured |
| INVALID\_DOC | Document validation (after signing) failed |
| UNKNOWN\_PROFILE | Unknown signature profile |
| EMPTY\_PARAM | Empty (null) parameter in request |
| INVALID\_TOKEN | Invalid token in request |
| PARSE\_ERROR | Couldn't parse request |

## 3.5. PDF visible signatures

For PDF signing, it is possible to create visible a signature field or to use an existing one.

There are quite a number of options (image, text, colors, ..) that can be specified. Because the token is limited in size it has been decided to use a ‘**PDF signature profile**’ file (see below) that is to be uploaded to the S3 server to hold most of the parameters and only provide a minimum of parameters in the **getTokenForDocument** call.

**1. So the getTokenForDocument call (and therefore the token) can only contain these parameters:**

* **psp**: the name of the ‘PDF signature profile’ file
* **psfN**: the name of an existing PDF visible signature field
* **psfC**: the ‘coordinates’ for a new PDF visible signature field, this is either
  + the string “default” to use the default coordinates that are specified in the ‘PSP’ file
  + a comma-separated value of 5 integers: *page*, the *x* and *y* coordinates, *width* and *height*
* **psfP**: a boolean, if true then the photo from the eID card is read and used as image
* **lang**: the language to be used for the text in the signature field, this language must be specified in the “texts” field of the PSP file

All parameter are optional, if none are specified then an invisible PDF signature is made.  
If psfN or psfC (they are mutually exclusive) are specified then a visble PDF signature is made/used.

This is an example of the contents of a getTokenForDocument request:

|  |
| --- |
| *{*  *"name":"minfin",*  *"pwd":"U84SnLEQvp",*  *"in":"test.pdf",*  *"out":"signed\_test.pdf",*  *"****psp****":"minfin1.psp",*  *"****psfC****":"1,20,30,180,60",*  *"****psfP****":true,*  *"****lang****":"en"*  *}* |

So the *psfC* value means: put a signature field on the **1**st page, at coordinates (**20**, **30**) from the left top corner of the page, with width **180** and height **60**

**2. The PSP (PDF signature profile) file is a json file as in the example below:**

|  |
| --- |
| {  "bgColor" : "#D0D0D0",  "texts" : {  "en" : "Signed by %gn% %sn%",  "de" : "Unterzeichnet von %gn% %sn%",  "nl" : "Getekend door %gn% %sn%",  "fr" : "Signé par %gn% %sn%"  },  "font": "freescpt",  "textSize" : 14,  "textPadding" : 20,  "textAlignH" : "CENTER",  "textAlignV" : "MIDDLE",  "textPos" : "BOTTOM",  "textColor" : "#0000FF",  "defaultCoordinates" : "1,30,20,120,60",  "imageDpi" : 400,  "image" : "ZGVmYXVsdA=="  } |

Remark: this profile json file is optional, if not present then default values are taken

The “bgColor” and “textColor “values for the RGB color code scheme, e.g. “#0000FF” = blue.

The “texts” can contain the following macros:

* **%gn%** : this is replaced by the Given Name in the user’s certificate
* **%sn%**: this is replaced by the Surname in the user’s certificate
* **%rrn%**: this is replaced by the RRN in the user’s certificate
* **%d(XXX)%**: this is replaced by the signing date, XXX is according to Java’s SimpleDateFormat [4]  
  e.g. %d(“d MMMM yyyy)% is replaced by e.g. “4 March 2021” in English

For the “font”, a number of fonts will be installed and their names documented. Currently there is the DSS default font and a “freescpt” font that resembles handwriting.

The “textAlignH” is the horizontal text alignment and can be “LEFT”, “CENTER”, “RIGHT”  
Default value is “NONE”, see [5]

The “textAlignV” is the vertical text alignment and can be “TOP”, “MIDDLE”, “BOTTOM”   
Default value is “NONE”, see [6]

The “textPos” defined the position of the text relative to the image: “TOP”, “BOTTOM”, “LEFT”, “RIGHT”

The “image” is a base64 image, the type (png, jpg, …) is automatically detected;  
or it can be the base64 encoding of the word “default”: "ZGVmYXVsdA==".

In case the “psfP” parameter is set to *true* in the getTokenForDocument call, then the photo of the eID card is used and the “image” value in the PSP is ignored.

All values are optional; in case of absence a default is used. If no “image” is specified then no image is used.

**3. Example query parameters in the redirect URL to BOSA**

* psfN=signature\_1 # PDF signature field name
* psfC=1,200,50,300,50 # PDF signature field coordinates: page,x,y,width,height
* psfP=true # if the photo should be read from the eID and used in the signature field

(this is because the token can't be parsed by the front-end)

Remarks:

* psfN and psfC cannot be used together
* In case of psfN, the PDF should contain a visible signature field with this value
* If (a) visible signature field(s) is/are present, then either psfN or psfC must be specified

**4. Current restrictions:**

* With the default font, the “textSize” parameter seems to be ignored
* The “freescpt” font is not by default installed on Linux
* When the image is on top or below the text, it expands or contracts horizontally in order to take the full width

## 3.6. Disabling downloads

Normally, the user signing the document is will be offered the signed version of the document at the end of the signing process. In case this is not desired, a “noDownload” parameter may be added to the “getTokenForDocument” call, with its value set to “true”:

|  |
| --- |
| {  *"name": "minfin",*  *"pwd":"U84SnLEQvp",*  *"in":"test.pdf",*  *"out":"signed\_test.pdf",*  ***"noDownload": true,***  } |

A document signed in this way will still be uploaded to the BOSA S3 service, but its signed version will not be made available to the user through the BOSA signing service.

Please note that only the download of the *signed* version will be blocked. The *unsigned* version *will* still be made available, because the user needs to know what they are signing.

## 3.7. Request a specific language when calling the service WEB UI

***private static String LANGUAGE = "en";*** *// options: en, nl, fr, de*

*// 3. Do a redirect to the BOSA DSS front-end*

*// Format:* ***[Fout! De hyperlinkverwijzing is ongeldig.](https://%7Bhost:port%7D/sign/%7Btoken%7D?redirectURL=%7BcallbackURL%7D&language=%7Blanguage%7D)***

*System.out.println("\n3. Redirect to the BOSA DSS front-end");*

*String callbackURL = localUrl + "/callback?filename=" + outFileName;*

*System.out.println("  Callback: " + callbackURL);*

***String redirectUrl = bosaDssFrontend + "/sign/" + URLEncoder.encode(token) +***

***"?redirectUrl=" + URLEncoder.encode(callbackURL) + "&language=" + LANGUAGE;***

## **3.8. Using XLST file**

*// 2. Do a 'getToken' request to the BOSA DSS*

*String json = "{\n" +*

*" \"name\":\"" + s3UserName + "\",\n" +*

*" \"pwd\":\"" + s3Passwd + "\",\n" +*

*" \"in\":\"" + inFileName + "\",\n";*

*if (null != xsltFile)*

***json += ( " \"xslt\":\"" + xsltFile.getName() + "\",\n" );***

*json += " \"out\":\"" + outFileName + "\",\n" +*

*" \"prof\":\"" + profileFor(inFileName) + "\"\n" +*

*"}";*

# 3. Sample/test FPS code and service

A simple Java service has been made that can serve as an example for the FPS.

It provides a simple ‘home page’ where the use can select a document to sign.  
Then the sample service uploads this document, requests a token and does a redirect.  
Finally a callback page is foreseen where the signed document is downloaded and the unsigned and signed document are deleted from the S3 server.

To build the sample: install maven and type the following on a command prompt:  
 *mvn package*

To run the sample service on Linux/MacOSX:  
 *java -cp "target/lib/\*":target/test\_fps-0.0.1-SNAPSHOT.jar com.zetes.projects.bosa.testfps.Main*Or on Windows:  
 *java -cp "target/lib/\*";target/test\_fps-0.0.1-SNAPSHOT.jar com.zetes.projects.bosa.testfps.Main*

When started successfully, the service will show the URL to which to surf to:

|  |
| --- |
| *Service started - press Ctrl-C to stop*  *Surf with your browser to http://localhost:8080* |

When the service starts, it reads configuration parameters from the ***config.txt*** file.  
*To actually be able to connect to the BOSA S3 service, an account should be requested from BOSA; and this account information (username and password) must be filled in this config file (i.e. replace the USERNAME\_HERE and PASSWORD\_HERE strings).*

**Demo service**

The above code has been deployed and can be found at the following URL: [3].

# References

[1] MinIO: <https://en.wikipedia.org/wiki/MinIO>

[2] MinIO SDKs: <https://docs.minio.io/> - select ‘MINIO SDKS’ on the left

[3] Sample/test FPS service: [https://mintest.qa.fts.bosa.belgium.be](https://mintest.qa.fts.bosa.belgium.be/)

[4] <https://docs.oracle.com/javase/7/docs/api/java/text/SimpleDateFormat.html>

[5] <https://ec.europa.eu/cefdigital/DSS/webapp-demo/apidocs/eu/europa/esig/dss/enumerations/VisualSignatureAlignmentHorizontal.html>

[6] <https://ec.europa.eu/cefdigital/DSS/webapp-demo/apidocs/eu/europa/esig/dss/enumerations/VisualSignatureAlignmentVertical.html>