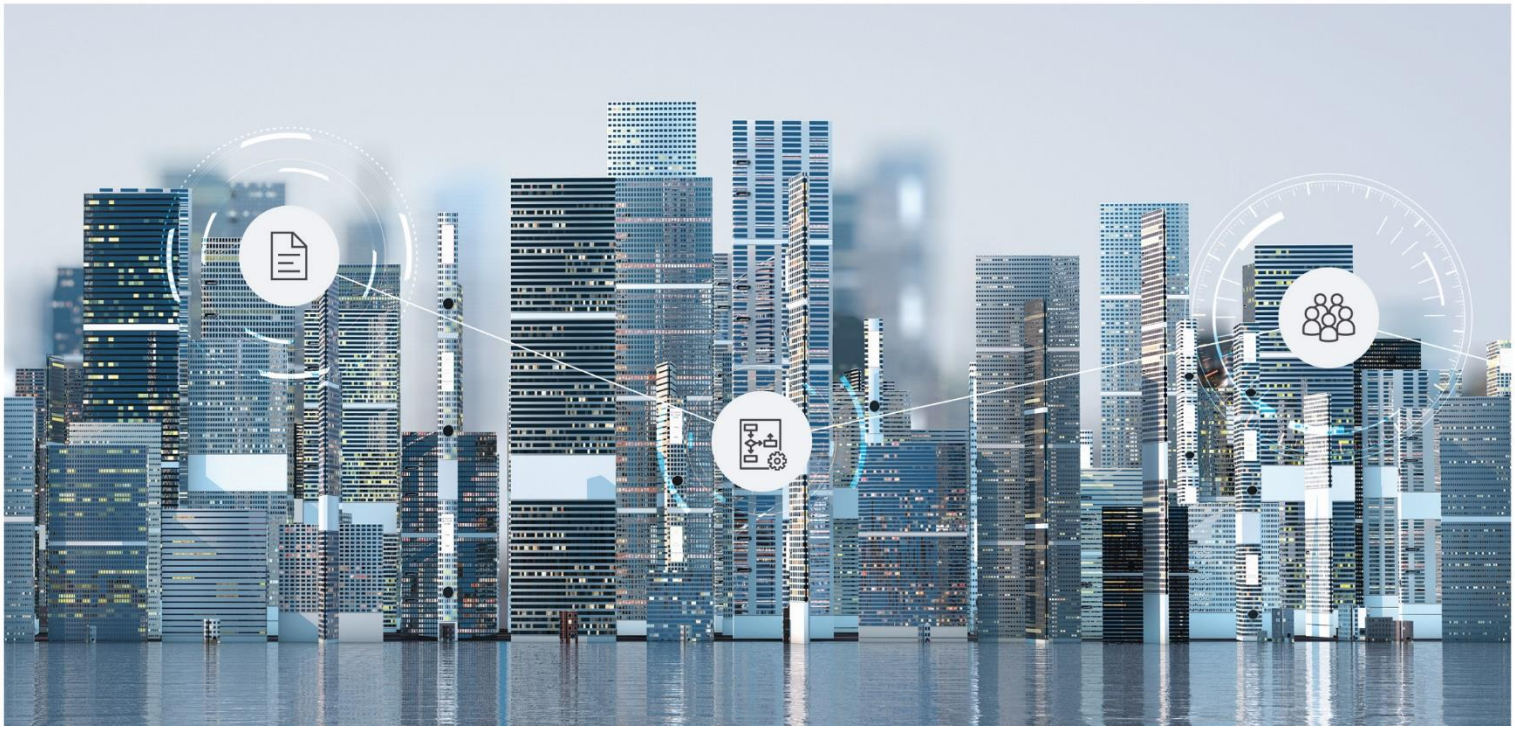
Fabasoft



White Paper

Digital Signatures in the Fabasoft Cloud

2023 March Release

Contents

1 Introduction

In the Fabasoft Cloud, documents can be signed digitally with a certificate, resulting in an PDF signature according the PDF standard ISO 32000-1:2008. This document describes the process of how the signatures are applied to documents, the administrative use cases to configure this functionality, and the technical details of these signatures.

For digital signatures, the following criteria are of special interest:

- Subsequent change of the document is detectable
  Digital signatures in the Fabasoft Cloud make use of PDF signatures that are based upon an asymmetric cryptographic system using signing certificates with public/private key pairs. Due to modern hashing and signature algorithms (SHA512, RSA-4096), subsequent changes in the document can be detected when validating the signature in an appropriate PDF viewer.
- High level of confidence in the signature creation system and in the protection of the signature creation keys
  The Fabasoft Cloud uses Fabasoft Secomo to generate the digital signature during the signing process. In Fabasoft Secomo, the private keys used for creating the signatures are stored in a highly secure manner, utilizing a hardware security module (HSM) that meets the requirements of FIPS 140-2 Level 4 physical security certification.
- Linking the signature to the signatory
  Each PDF signature is linked to exactly one signatory. These signatories are able to use their visual signature images when applying a digital signature. In that image, a hash of the globally unique ID of the user in the Fabasoft Cloud environment is generated (signatory identification), which will allow to verify whether the signature was applied by exactly that particular user. Moreover, the names of the signatories, the name of their organizations, the login e-mail address and the signatory identification are added to the so-called “signature reason” of the PDF signature so that the signatory can easily be verified directly in an appropriate PDF viewer. In addition to the identification data in the “signature reason” of the PDF signature, the underlying signature structure will also contain the login e-mail addresses and the user IDs of the signatories as well as the ID of the signed document in the Fabasoft Cloud. Although this additional identification data is not directly displayed in the PDF viewer, it can be checked by using special analysis tools as explained below.
- Authentication and identification of the signatory
  In the Fabasoft Cloud, signatories must authenticate themselves using various strong authentication methods (including 2-factor authentication). Hence, it is not possible to sign documents just because of receiving documents via e-mail.
  As mentioned above, the login e-mail address as well as the signatory identification are added to the “signature reason” so that you can see directly the identification data of the signatory when checking the signature data in an appropriate PDF viewer.

2 Applying Digital Signatures in the Fabasoft Cloud

This chapter describes the process of how a digital signature is applied to a document by a user in the Fabasoft Cloud.

2.1 Logging in as User in the Fabasoft Cloud

To apply a digital signature to a document, signatories must authenticate themselves in the Fabasoft Cloud. Various authentication methods, including 2-factor authentication, are available for

this purpose. Users and the available authentication methods are managed by the administrators of their cloud organization.

Either the web client or the “Fabasoft Cloud“ mobile app for iOS or Android can be used for signing documents.

2.2 Provide Images for Visual Signature

When digitally signing documents, users can insert visual representations of their respective signatures. In order to do so, the user can define images in the settings menu (account menu (your user name)” > “Advanced Settings” > “My Signatures”). These images can either be uploaded as an image file, generated from an entered text, or created as handwritten signature at the workstation or on the mobile device.

When a visual signature is inserted in the signing dialog, an identification for the signatory (i.e. the current user) is automatically generated below the signature image. In the Fabasoft Cloud, each user can be identified by the *Fabasoft Cloud ID* (i.e. property with reference: `COOSYSTEM@1.1:objaddress`) of the object representing that specific user. The *Fabasoft Cloud ID* cannot be changed whereas the login e-mail address or the name of the user may change over time. The signatory identification is made up of the first 40 characters of the SHA256 hash of this *Fabasoft Cloud ID*.

Note: If a user has to be anonymized in the Fabasoft Cloud (e.g. due to data privacy reasons), it is not possible to find the *Fabasoft Cloud ID* of the original user anymore.

2.3 Close Documents

Documents must be closed (i.e. finalized) before signing them. When a document is closed that is not in PDF format, the document will be converted to the PDF format so that the PDF signature can be applied afterwards. When signing a document in the web client, it will be automatically closed before opening the signing dialog.

2.4 Open the Signing Dialog

The user starts the signing dialog either via an activity work item in the workflow or by selecting the corresponding menu entry from the context menu in the web client. In the mobile app for iOS or Android, the signing dialog can be opened only via the activity work item in the workflow.

2.5 Add Visual Signatures, Stamps, and Text Fields in the Signing Dialog

In the signing dialog, a user may place the following elements into the document:

- Images representing the visual signature of the user
  These visual signatures can be configured by the users themselves in the settings menu. The visual signature also contains the signatory identification.
- Images representing stamps of the organization
  These stamps are configured by the administrator of the cloud organization. A stamp will not contain the signatory identification.
- Text fields
  These fields may contain the name of the signatory, the place, a date, or any free text.

The signatory may add zero, one or multiple visual signatures, stamps, or text fields, and distribute them on multiple pages.

2.6 Add a Remark in the Signing Dialog

The signatory may add a remark for the signing operation in the signing dialog.

2.7 Select a Certificate for Signing in the Signing Dialog

If the administrator of the cloud organization has uploaded multiple certificates for signing, the user may also select one of these certificates which are then used to apply the PDF signature.

If there is no certificate configured for the cloud organization, a default certificate provided by the Fabasoft Cloud is used to apply the PDF signature.

This default certificate is issued for:

```
email=digitalsignatures@fabasoft.com, cn=Fabasoft Business Process Cloud Digital
Signatures, ou=Cloud Service, o=Fabasoft AG, l=Linz, st=Oberösterreich, c=AT
```

It is issued by the following trusted certificate authority:

```
cn=GLOBALTRUST 2020 AATL 1, o=e-commerce monitoring GmbH, c=AT
```

2.8 Applying the PDF Signature

All data entered in the signing dialog will be transferred to the server of the Fabasoft Cloud. On the server, the PDF signatures will be applied to the PDF document.

Multiple PDF signatures may be created because

- the user added visual signatures, stamps, or text fields on multiple pages.
- the user added multiple visual signatures or stamps on a page.

For each PDF signature, the following steps will be executed:

- The remark (if provided), the name of the user, the name of the organization, the login e-mail address, and the signatory identification will be stored in the *signature reason* property of the PDF signature.
- "Fabasoft Cloud" will be stored in the *signature location* property of the PDF signature.
- The digital signature for the PDF document and some additional information is generated by Fabasoft Secomo where the private key of the certificate is stored, secured by a hardware security module (HSM).
- The PDF signature is stored in the PDF document.

For further information, refer to chapter 4 "Technical Details".

In addition to the PDF signature, each signing operation will be protocolled in the meta data of the signed object. Open the properties of the object and switch to the "Signatures" tab. On that tab, you will see all electronic signature operations, all digital signature operations, and the signing times, the remarks, and the user objects that have applied the signatures.

3 Administering the Digital Signature Functionality in the Fabasoft Cloud

This chapter explains the administration use cases related to digital signatures. These use cases can only be executed by administrators or owners of the cloud organization.

3.1 Adding Certificates to a Cloud Organization

To enable the digital signing of documents with custom certificates, administrators of the cloud organization can store the corresponding certificates in their organizations ("Advanced Settings" > "Configure Digital Signatures" action).

The administrator has to upload an X.509 certificate in PKCS #12 file format including the private key. Moreover, the certificate password to extract the private key must be defined.

The uploaded certificate is securely transferred to Fabasoft Secomo where it is stored securely by a hardware security module (HSM) that meets the requirements of FIPS 140-2 Level 4 physical security certification. In the Fabasoft Cloud, only the public information of the certificate is stored.

For each uploaded certificate, the administrator can specify which organization members are allowed to use this certificate in the signing dialog.

Note:

- If the use of X.509 certificates is restricted, one of the following usage types ("Key Usage") is required: "Digital Signature" or "Non Repudiation".
- Certificates can be updated using the context menu command "Update". Organization administrators and owners receive a notification on the welcome screen as soon as the certificate expires within the following two weeks or has already expired.
- Certificates can be deleted using the context menu command "Delete". Deleted certificates can no longer be used for signing, but already signed documents are not affected.

3.2 Adding Stamps to a Cloud Organization

In addition to certificates, the administrator can also define stamps ("Advanced Settings" > "Configure Digital Signatures" action). For each uploaded stamp, the administrator can specify which organization members are allowed to use this stamp in the signing dialog.

4 Technical Details

In this chapter, you can find technical details about how the digital signature within the Fabasoft Cloud is applied to stored documents.

4.1 File Format

The Fabasoft Cloud can automatically convert a huge number of native file formats (e.g. Microsoft Office documents) to PDF. Whenever you trigger the digital signature of a document inside the Fabasoft Cloud (either via the corresponding context menu entry or its related activity work item), the PDF representation of the document is finalized. This means that the properties of the Fabasoft Cloud object holding the document are set so that the document cannot be changed any further and its document is converted to PDF/A. Details related to the PDF file format can be found in the corresponding specification PDF 1.7 (ISO-32000-1:2008).

4.2 Digital Signature

Digital signatures applied to documents within the Fabasoft Cloud follow the specifications defined within the PAdES standard (ETSI EN 319 142 PAdES digital signatures) published by the ETSI (European Telecommunication Standards Institute).

In preparation to apply the signature to the document, a so-called visual signature stream (a special PDF data structure that contains the visual representation of the digital signature) is prepared. The stream is assembled from the applied text fields (like signatory's name, location, date, and free text fields), the image of the selected visual signature, or the selected stamp. The *signature reason* string will be assembled from the remark (if provided), the name of the user, the name of the organization, the login e-mail address, and the signatory identification. The *signature location* will be set to "Fabasoft Cloud" and the *signature time* will be set to the current time of the server.

Next, an SHA512 digest of the underlying PDF/A compatible document, including the signature streams with the visual signatures, the signature reason, the signature location and signature time, is calculated.

This SHA512 digest is securely sent to Fabasoft Secomo. The current Fabasoft Cloud user context is passed to Fabasoft Secomo by means of a signed JSON Web Token (JWT) that includes the login e-mail address and the Fabasoft Cloud ID of the current user, the Fabasoft Cloud ID of the signed object, and optionally the Fabasoft Cloud ID of the organization that provides the signing certificate.

Fabasoft Secomo calculates signatures according the Crypographic Message Syntax (CMS) standard (IETF RFC 5652) and the CAdES standard (ETSI EN 319 122 CAdES digital signatures) based on the given digest and the corresponding private key of the signing certificate which is secured within Fabasoft Secomo by a hardware security module (HSM) that meets the requirements of FIPS 140-2 Level 4 physical security certification. The signature algorithm RSA-4096 is used for the signature. Fabasoft Secomo will also add the identification data from the JWT to the signed CMS structure (i.e. the login e-mail address and the Fabasoft Cloud ID of the current user, the Fabasoft Cloud ID of the signed object, and optionally the Fabasoft Cloud ID of the organization that provides the signing certificate).

Afterwards, the DER-encoded signature data is returned and embedded in the PDF document according to the PAdES standard to keep the source document unchanged.

Due to this "Envelop Embedding Approach" multiple Fabasoft Secomo signatures can be applied, one after the other. All the preceding signatures are part of the base document for the next signature. This means that each individual signature envelopes the entire base document without changing it.

Keeping the original document unchanged is a key requirement to validate signatures at a later time.

If more than one signature is applied in the same step, every signature image (visual signature or stamp) triggers a separate signature as if they were done sequentially.

4.3 Checking the Signatory Identification

If you want to check the signatory identification, retrieve the *Fabasoft Cloud ID* from the user object you want to check, and calculate the SHA256 hash from it. For example, you can use the open source software OpenSSL to do so:

```
echo -n "COO.6505.100.1.15" | openssl dgst -sha256
```

4.4 Checking the CMS Structure

The signature reason will be displayed in appropriate PDF viewers. However, under normal circumstances, PDF viewers do not show the data encoded in the CMS structure. Here are some tools that will allow you to analyze the CMS structure, too.

1. You need a tool that will give you access to the CMS structure in the PDF document. You may use the open source software PDFBox (https://pdfbox.apache.org/download.html) for that.
   `java -jar pdfbox-app-<version>.jar PDFDebugger`
2. Open the PDF file and choose "View" > "Show Internal Structure".
3. You should find the signature content under "Root" > "AcroForm" > "Fields" > [index] > "V" > "Contents".
4. Copy the hexadecimal content to a file and convert it to binary format.
   `xxd -r -p signature.hex signature.bin`
5. Display the CMS structure with OpenSSL.
   `openssl cms -in signature.bin -inform DER -cmsout -print`

Note:

- The additional identification data is stored in the attribute `signer-attributes-v2` (OID `0.4.0.19122.1.1`, defined by ETSI in the CAdES Standard).
- The attribute with OID `1.3.6.1.4.1.17100.2.6` contains the "Domain ID" of the Fabasoft Cloud location.
- The attribute `emailAddress` contains the login e-mail address of the signatory.
- The attribute with OID `1.3.6.1.4.1.17100.2.5` contains the Fabasoft Cloud ID of the user object representing the signatory.
- The attribute with OID `1.3.6.1.4.1.17100.2.1` contains the Fabasoft Cloud ID of the organization object that provides the signing certificate. If the default certificate was used for signing, the attribute is empty.
- The attribute with OID `1.3.6.1.4.1.17100.2.4` contains the Fabasoft Cloud ID of the signed document.

4.5 Restrictions

Since the Fabasoft Cloud does not use personalized certificates by default, the name of the signatory, the organization, the login e-mail address, and the signatory identification are set in the *signature reason* property (optionally textually combined with the user entered remark) of the PDF signature options when signing the document. In addition, the CMS signature structure also contains the login e-mail address and the unique Fabasoft Cloud ID of the user object that applied the signature. This helps to ascertain which user applied the signature although there is no binding of a person to one specific and personally issued certificate.

The time of the signature will be retrieved from the server of the Fabasoft Cloud. A timestamp service is not used. The applied signature does not allow long-term validation (LTV). In order to validate the signature successfully, Internet access is required to load the revocation information from the certificate authority.