Certificates and Signatures

Administration Tool

Table of contents

Requirements for signature

Signature-specific license

The signature functions described in the present document are not included by default in all Gargantua installations: therefore, if you want to benefit from them, your organization needs to acquire a specific license, so that you have access to the **Certificates** branch in the Administration Tool and to all related functions.

Requirements for the use of USB eTokens

Installing SafeNet Authentication Client

The eToken signature functions included in Gargantua 7 rely on strong authentication solutions developed by SafeNet (www.safenet-inc.com).

Therefore, to be able to sign documents using USB eTokens, you must:

- As far as software is concerned, install SafeNet Authentication Client on every workstation;
- As far as hardware is concerned, use the corresponding USB eToken keys.

To install SafeNet Authentication Client, proceed as follows:

1. In the installation kit provided by SIATEL, find and launch the following file: SafeNetAuthenticationClient_x32_x64_8.00-SP1.exe (**SafeNetAuthenticationClient8_0_SP1** > **32X64 Installer**).

   The setup wizard displays.

2. Click **Next**.
3. In the drop-down list, select the appropriate language, then click **Next**.
4. Select the radio button **I accept the license agreement**, then click **Next**.
5. Select the **Standard** installation type, then click **Next**.
6. Select the folder on your hard drive where you want to install the application: you can either leave the default or choose another folder using the **Browse** button.
7. Click **Next** in order to launch the setup, then wait until a success message displays.
8. Click **Finish**.

   SafeNet Authentication Client is now installed on the workstation: you can use USB eTokens to sign documents within Gargantua.

Using SafeNet Authentication Client

The user guide for SafeNet Authentication Client is included in the installation kit provided by SIATEL (**SafeNetAuthenticationClient8_0_SP1** > **Documentation** > **SAC_User_Guide_8.0_SP1_Windows_Rev_A.pdf**).

When using SafeNet Authentication Client with Gargantua, you will probably need to know how to perform the following operations:

- How to import certificates to the USB eToken: see “Importing a Certificate Onto a Token”, p. 46 of the SafeNet user guide;
- How to export certificates from the USB eToken: see “Exporting a Certificate from a Token”, p. 50;
- How to delete certificates from the USB eToken: “Deleting a Certificate”, p. 54;
- How to change the password for the USB eToken: “Changing the Token Password”, p. 36.

Gargantua signature features

Types of signatures

A Gargantua signature can be digital (visible or invisible) and/or handwritten. The following combinations are possible:

- The **digital signature** allows you to sign a document using a digital certificate.
- The **visible digital signature** allows you to sign a document using a digital certificate that will be visible directly in the body of the PDF document.
- The **handwritten signature** allows you to sign the document using a signature image file, and no digital certificate.
- The **handwritten and digital signature** allows you to combine a signature image file with a digital certificate.
- The **handwritten and visible digital signature** allows you to add a signature image file and a visible digital certificate that will be visible directly in the body of the PDF document.

Digital signature

Digital signature allows you to **apply a digital certificate** on a document.

A digital certificate is a file that contains:

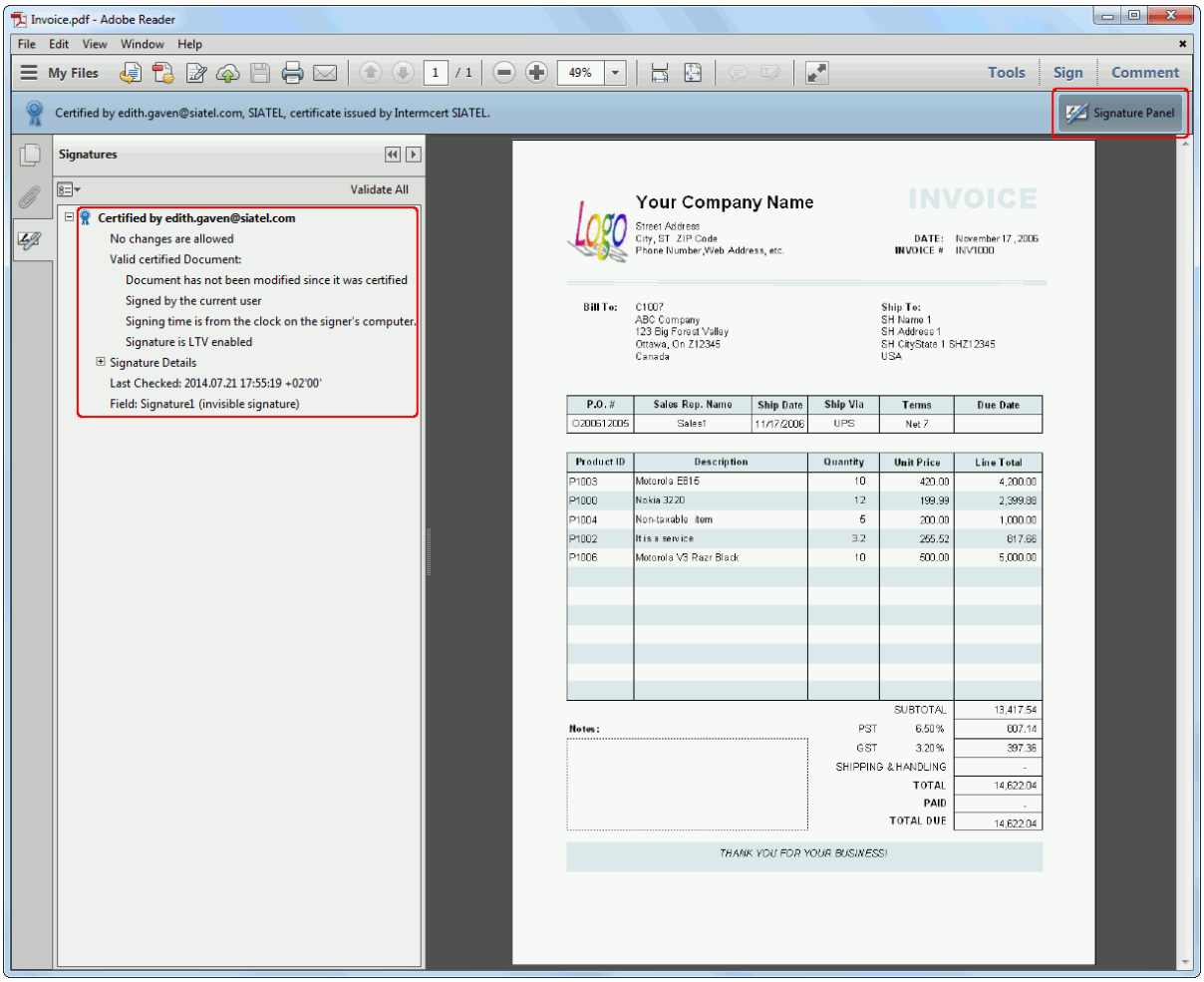
- A set of information about its owner's identity (name, address...);
- Two encryption keys:
  - A private key allowing the owner of the certificate to add it to digital documents by entering the certificate password;
  - A public key allowing the recipients to make sure that the certificate and, therefore, the documents are genuine.

Digital signatures are usually validated by trusted **Certification Authorities** (CAs) like VeriSign, specialized in generating and authenticating certificates. Still, organizations can also create **their own internal Certification Authorit**y to generate self-signed certificates for internal purposes.

The digital signature functions in Gargantua allow for both scenarios. You can:

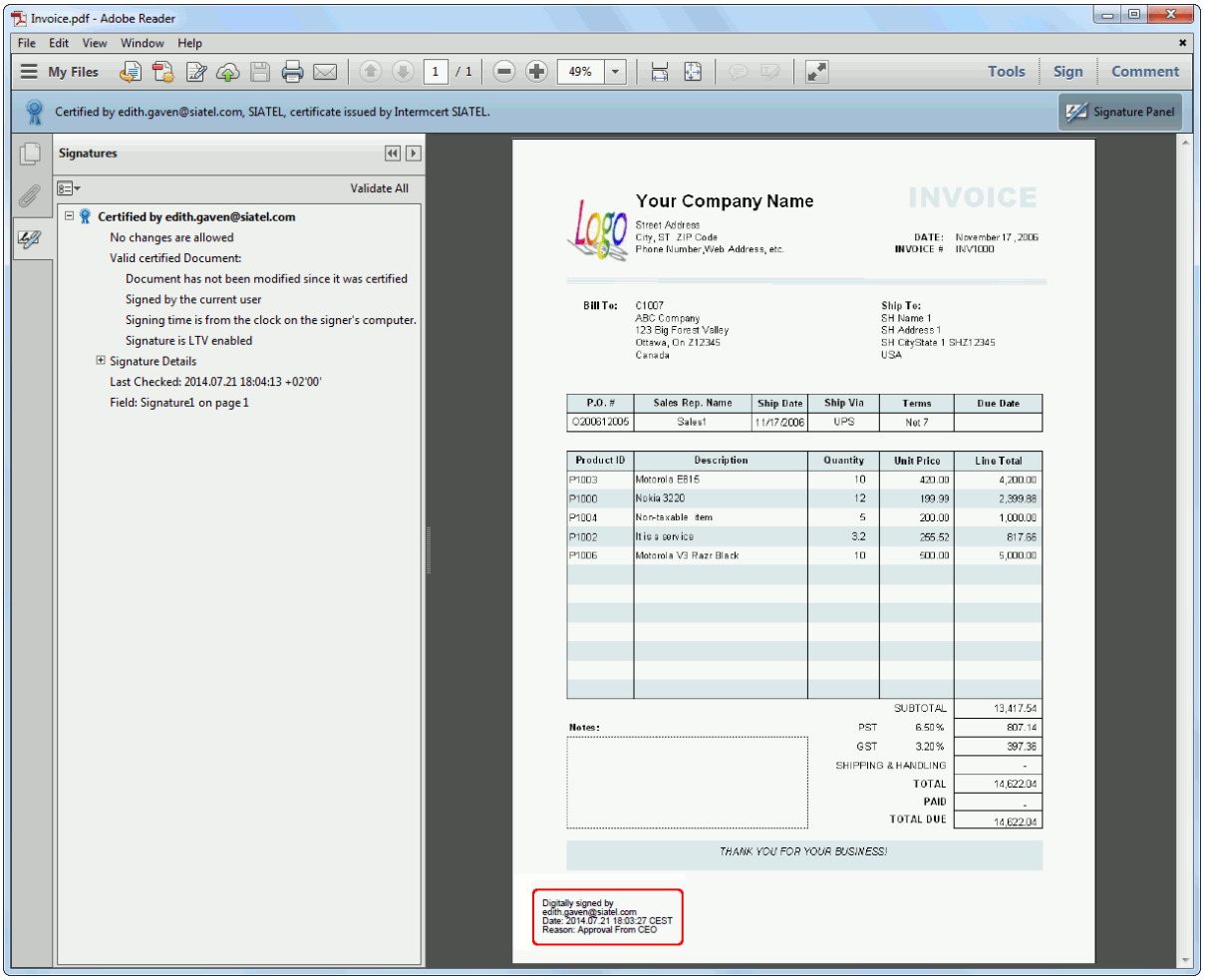
- Sign documents using digital certificates in .p12 or .pfx format delivered by trusted CAs;
- Create one's own CA on the Gargantua server in order to generate self-signed user certificates.

When a document is signed using Gargantua's digital signature functions, it is converted to PDF format. The information about the certificate's owner and authenticity can then be accessed through the **Signature Panel** in Adobe Acrobat Reader:



Visible digital signature

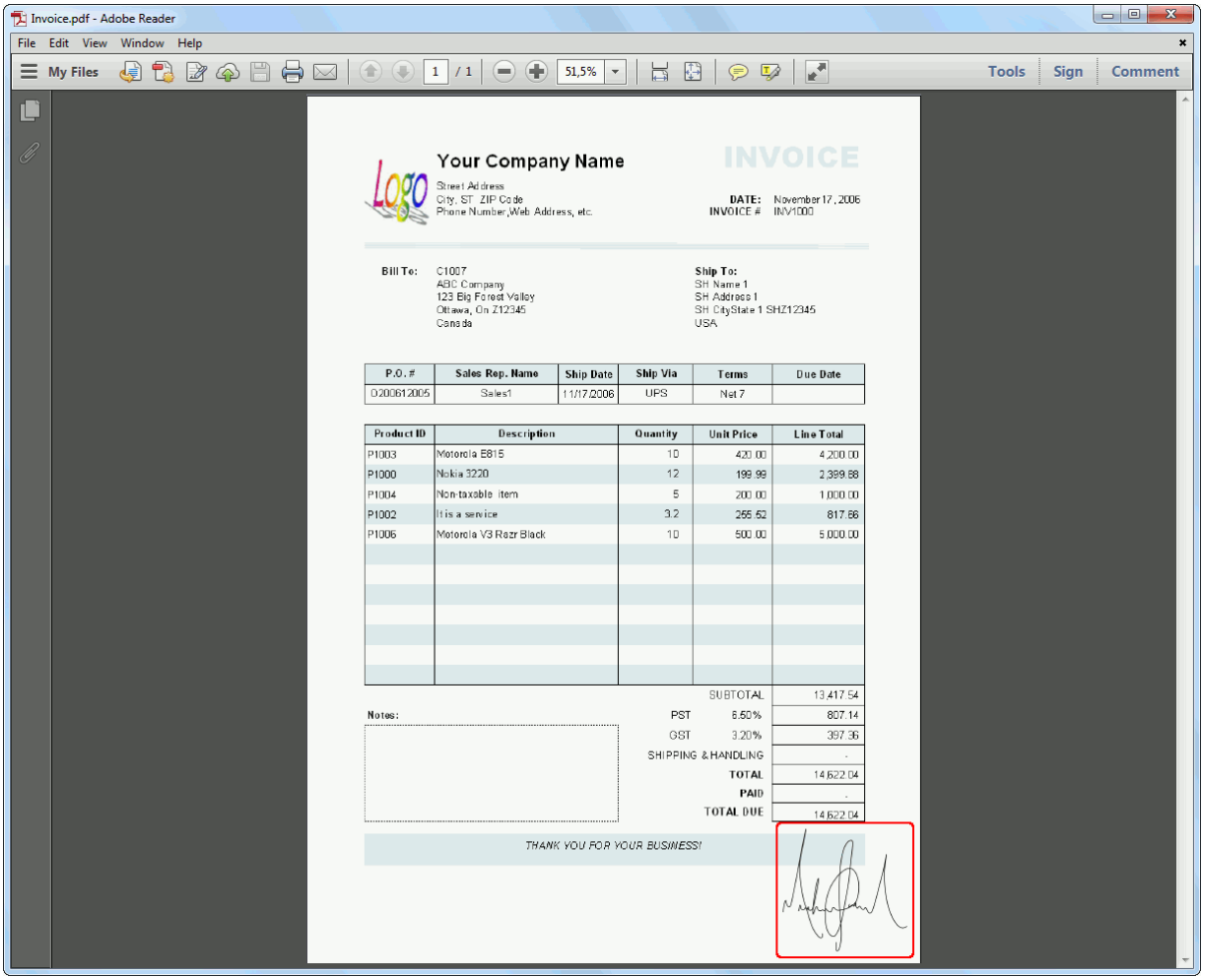
A digital signature is always available in Adobe Acrobat Reader's **Signatures panel**. However, if you want the signature to be **visible directly on the body of the PDF document**, you can use Gargantua's visible digital signature function:



When adding the signature, the Gargantua Web Client user can choose in which page and where in the page the signature will be visible.

Handwritten signature

The handwritten signature allows you to add a signature **from an image file**. It can also be combined with a digital signature:



Types of digital certificates

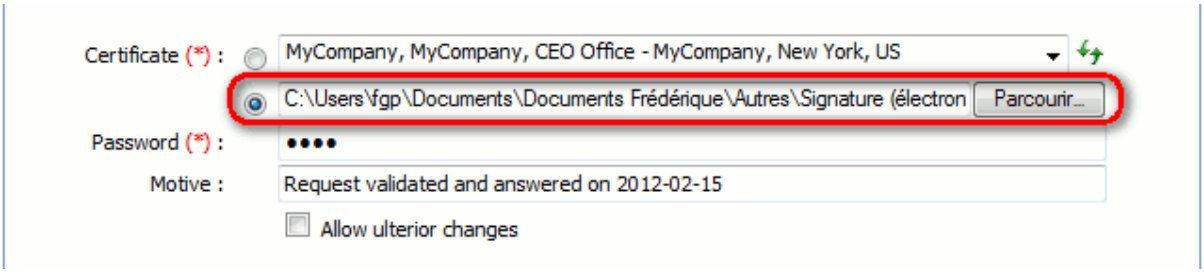
When adding a digital signature (visible or not), users can choose between three types of digital certificates.

> ***To access the digital signature, users need to select the appropriate documents, and then click the "Add a digital signature" tool or the "Add a visible signature" tool (not including the "Handwritten signature" option).***

Certificate stored locally

The users of Gargantua Web Client can add a digital signature to one or more documents using a .p12 or .pfx

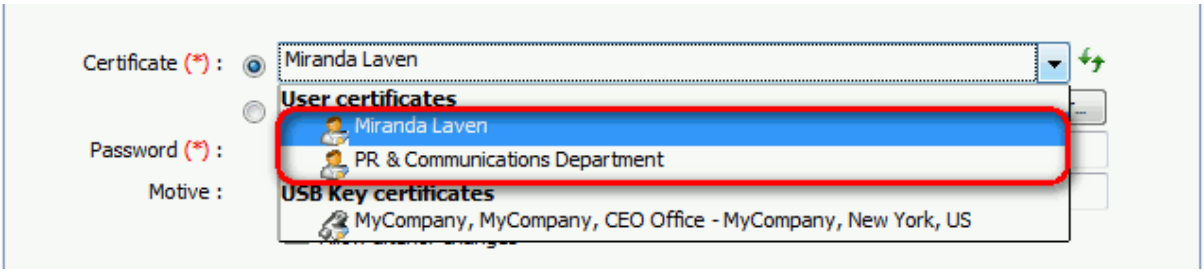
certificate file stored in their hard drive:



Certificate stored on the server

Alternatively, users of the Web Client can sign one or more documents using digital certificates stored on the Gargantua server and assigned to them.

The certificates available for the current user display in a drop-down list in the **Certificate** drop-down list:

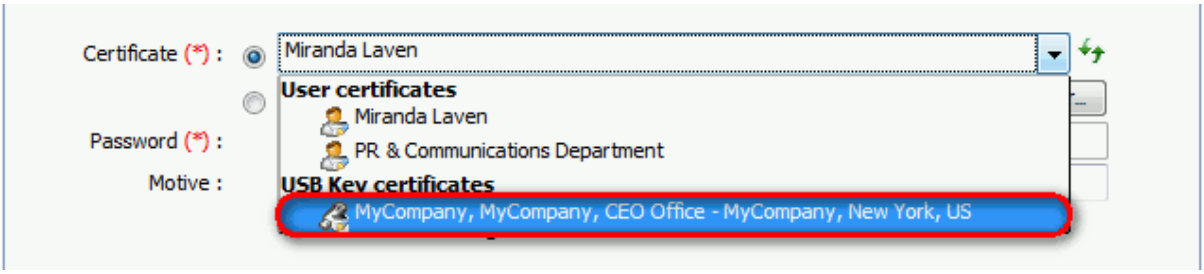


This method offers two main advantages: first, it makes certificates available for the appropriate users from any workstation; secondly, it protects the certificates against theft.

Certificate on USB eToken

Users of Gargantua Web Client can sign documents digitally using certificates stored on a USB eToken (see Requirements for the use of USB eTokens).

To do this, users need to connect the USB eToken to their workstation and enter its password. The drop-down list of all certificates available to the current user is then updated, so that it includes the certificates stored on the eToken:



Signature methods

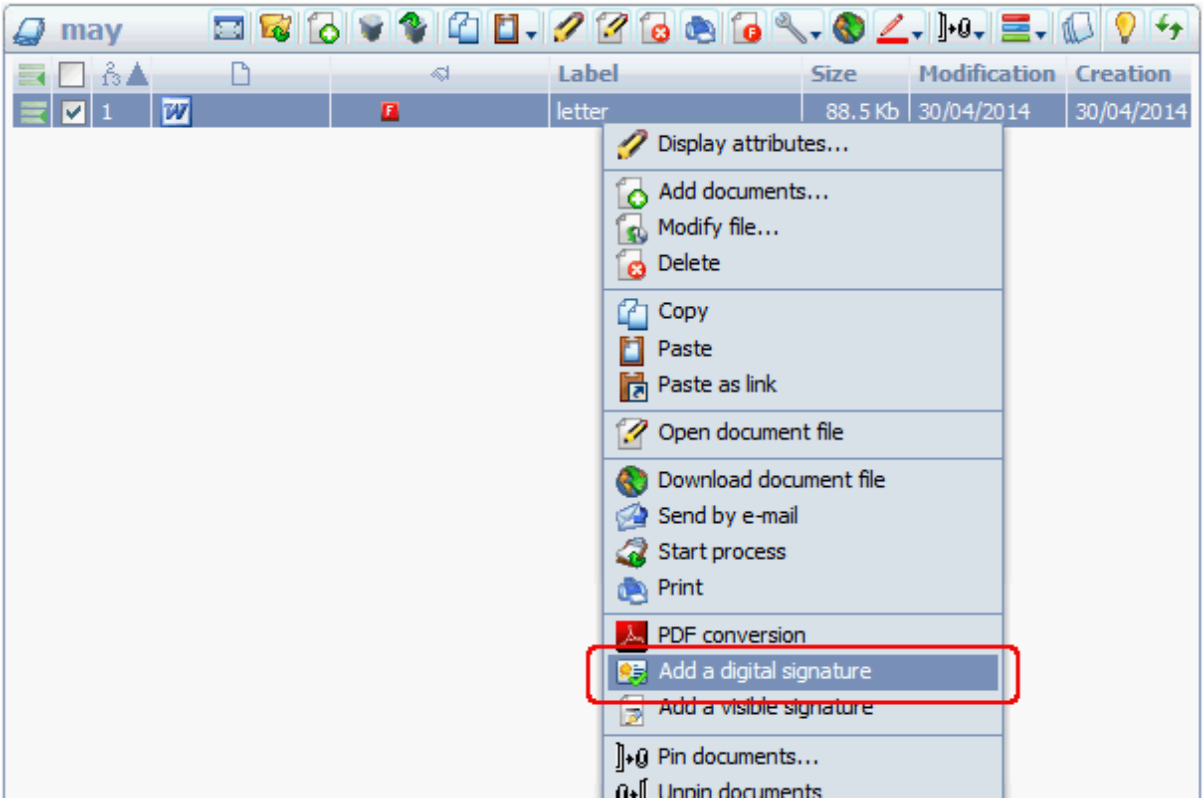
Gargantua allows you to sign documents manually directly on a browser, using the Add a digital signature or Adda visible signature tools; or automatically using a signature workflow task.

Manual - "Add a digital signature" tool

The **Add a digital signature** tool allows you to sign documents using only a digital certificate, **invisible** on the PDF document body.

> ***To use this tool, users need to have been granted the "Add a digital signature" access right (security profiles) on the documents.***

This tool can be used on several documents at a time.



MANUAL - "ADD A VISIBLE SIGNATURE" TOOL

The **Add a visible signature** tool includes all the available types of signatures that are visible in the body of the PDF document:

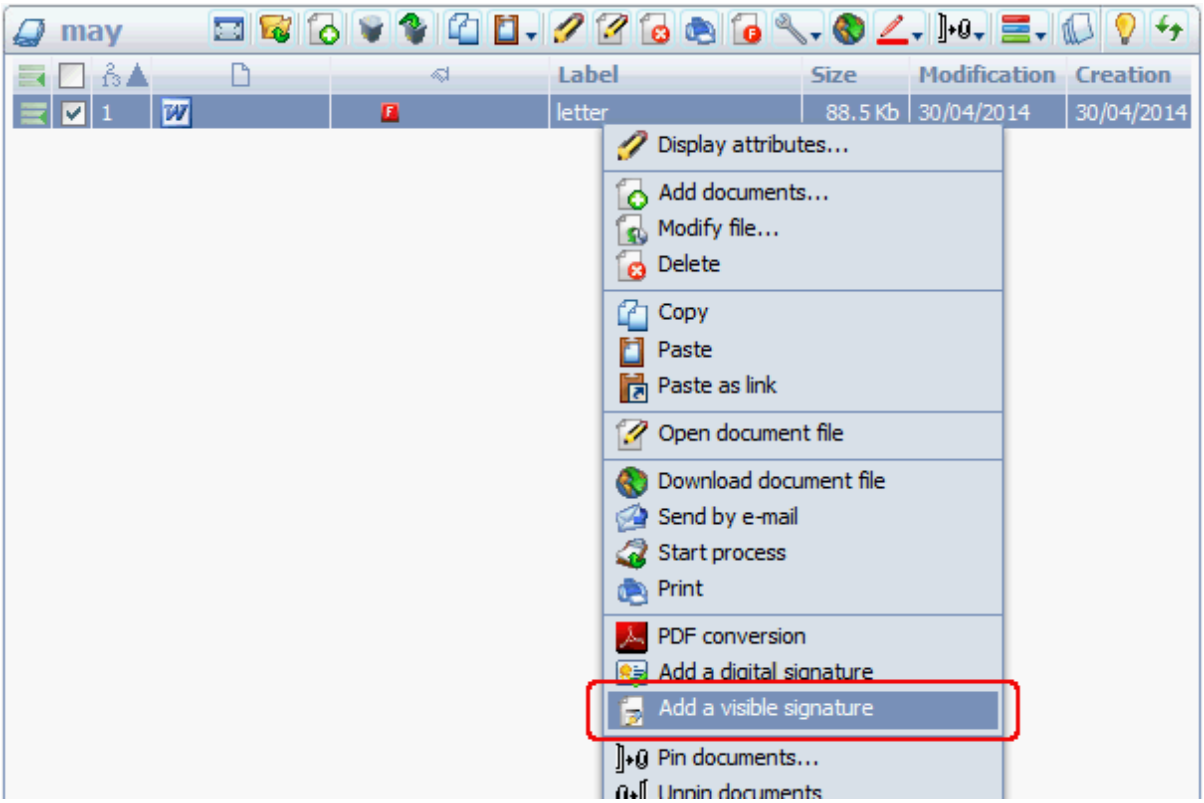
- The **visible digital signature** allows you to sign a document using a digital certificate that will be visible directly in the body of the PDF document.
- The **handwritten signature** allows you to sign the document using a signature image file, and no digital certificate.
- The **handwritten and digital signature** allows you to combine a signature image file with a digital certificate.
- The **handwritten and visible digital signature** allows you to add a signature image file and a visible digital certificate that will be visible directly in the body of the PDF document.

*For this tool to be available in the documents list toolbar, users need to have been granted the **"Visible signature"** privilege (manage users, groups or roles screens).*

*To use this tool, users need to have been granted the **"Add a digital signature"** access right (security profiles) on the documents.*

*To use this tool, a signature image must have been previously uploaded to the server (**"Settings"** > **"Signature and certificate settings"** > **"Handwritten signature"**).*

This tool can only be used on one document at a time.



AUTOMATIC - "DIGITAL SIGNATURE" WORKFLOW TASK

Documents can be signed automatically as part of workflow processes, using digital signature tasks.

To create and set up an automated digital signature task, proceed as follows:

1. In the left pane of Gargantua Administration Tool, expand the appropriate branches, and click the name of the process you want to insert a digital signature task into.

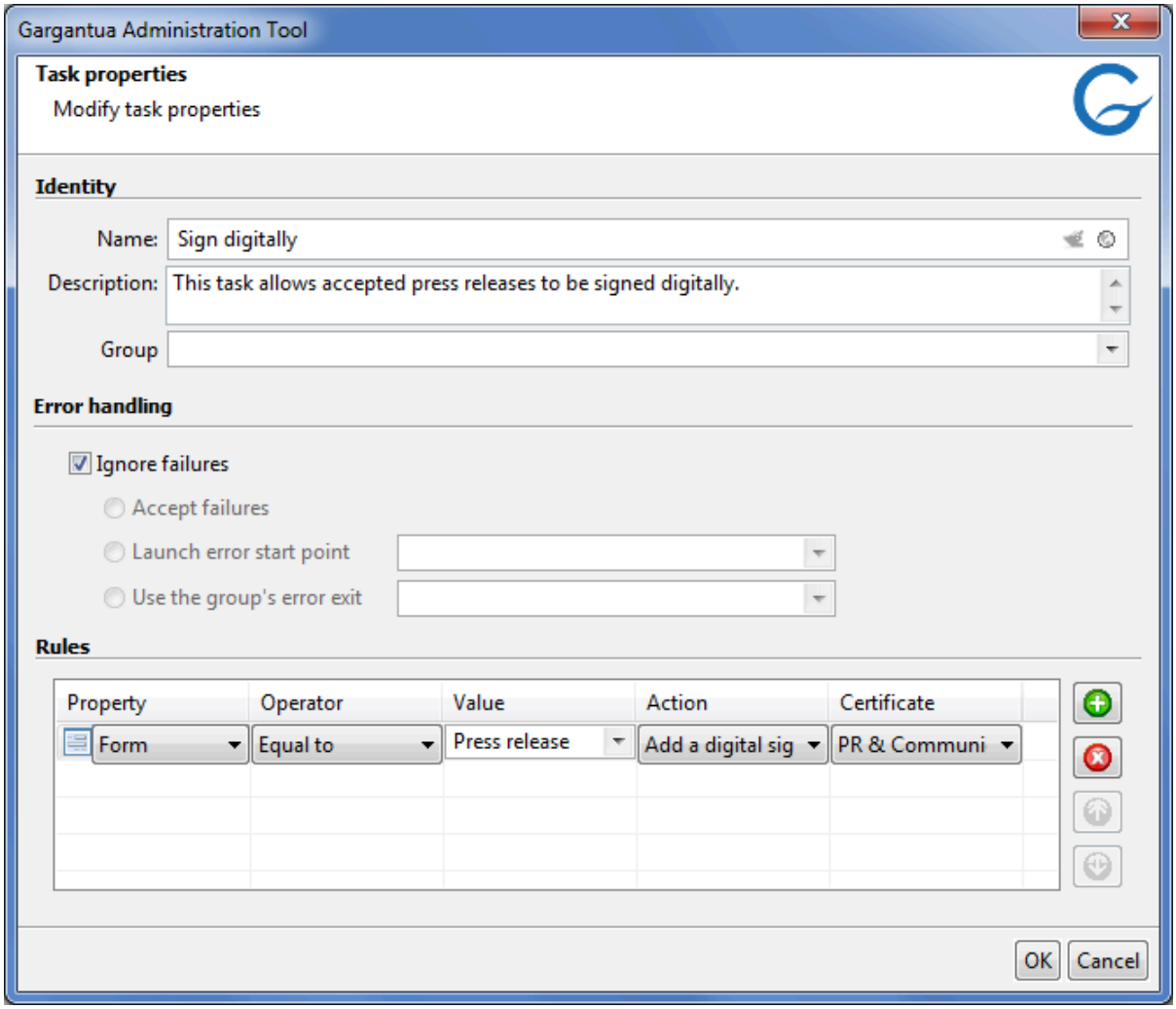
   The **Manage processes** screen displays in the right pane.

2. Unless the **Graph** tab is selected by default, click it.

3. In the toolbar, click the  icon and drag-and-drop it to the process designing area in order to create a new **Digital signature task**.

4. After adding the necessary edges, double-click the new  task.

   The **Task properties** dialog opens:



5. Enter a name and, optionally, a description for the task.
6. Add, if necessary, the task to a group.
7. Use the  button to create at least one rule specifying when and how the process documents should be signed:

   - **Property**: Select a criterion to sort the documents so you can decide whether a document must be signed or not. Possible criteria are the form used by the document, the type of the corresponding file (.doc, .tif, .txt...) or the contents of the **label** field of the form.
   - **Operator**: Choose the appropriate operator to evaluate the condition.
   - **Value**: Enter or select the value to which the document properties should be compared to

know if the condition is valid.

- **Action**: Select **Add a digital signature** (the **Encrypt** option allows you to convert the documents to encrypted PDF documents, so that they can be consulted in read-only mode, but neither modified nor copy-pasted.)
- **Certificate**: Select the certificate to use in order to sign the documents for which this condition is valid. Only server certificates are available here (see Assigning a certificate to one or more users).

> ***Each document can only be signed once, so that the different rules are mutually exclusive. If a document satisfies several conditions, only the first rule will be applied.***

8. If necessary, you can delete or reorganize rules using the  ,  and  button.
9. When you are done, click **OK** to close the dialog.

All the documents that satisfy the rules you have just set will now be signed automatically as part of the workflow process.

Managing certificates with Gargantua Administration Tool

Importing a certificate stored locally

The **Certificates** branch in Gargantua Administration Tool allows you to store and manage centrally on the server the certificates used by Gargantua users in order to authenticate the documents.

To upload a certificate stored on your hard drive to the server, proceed as follows:

1. In the left pane of Gargantua Administration Tool, click the **Certificates** branch.

   The **Manage certificates** screen displays in the right pane.

2. In the bottom right corner of the right pane, click the **Import** button.

   The file explorer displays.

3. Browse to the location where you have saved the certificate file, select it, and click **Open**.

   Imported certificate files must be in .p12 or .pfx format.

   A dialog displays.

4. Enter the password for the certificate, and click **OK**.

   A dialog displays.

5. Fill in the **Name** field; be careful to choose a name that makes it easy to identify the certificate in the **Certificates list** when imported.
6. If you want to assign the certificate to one or more users or natural persons, fill in the **Issued to** field.

   Else, if you want to use the certificate for digital signature tasks in workflow processes, check the **This is a server certificate** checkbox.

7. When you are done, click **OK**.

   The certificate has been imported to the server: it now appears in the **Certificates list**.

Users of the Web Client who have access to the "Settings" link can also upload certificate files to the server (Settings > Signature and certificate settings > User certificate settings). Those certificates then appear in the "Certificates list" in the Administration Tool, where they can be managed, reassigned, or even deleted, by administrators.

Creating an internal CA on the Gargantua server

If you do not want to buy a certificate issued by a trusted CA (Certificate Authority) for each of your users, Gargantua allows you to create your own CA on the server, in order to generate self-signed certificates for internal use.

To create your own CA using Gargantua Administration Tool, proceed as follows:

1. In the left pane, click the **Certificates** branch.

   The **Manage certificates** screen displays in the right pane.

2. In the lower part of the right pane, click the **Create my root certificate now** button.

   A dialog displays.

3. Enter the appropriate information, and click **OK**.

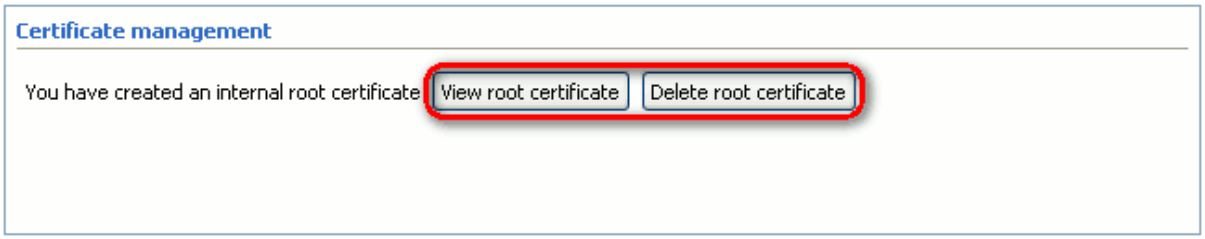
   A dialog displays.

4. Enter the password you want to assign to the root certificate, and click **OK**.

   Your internal CA has been successfully created.

   Two new buttons replace the **Create my root certificate now** button:

   - The **View root certificate** button allows you to consult the information associated with your CA;
   - The **Delete root certificate** button enables you to destroy your internal CA, along with **all related self-signed certificates**.



Creating self-signed certificates on the Gargantua server

After creating your own CA on the Gargantua server, you can start using it to generate self-signed certificates:

1. In the left pane of Gargantua Administration Tool, click the **Certificates** branch.

   The **Manage certificates** screen displays in the right pane.

2. In the bottom left corner of the right pane, click the **New** button.

The **New user certificate** dialog displays.

3. Enter the appropriate information. Be sure to:
    - Choose an explicit **Name** for your new certificate, so that you can identify it easily in the **Certificates list** when created;
    - Assign the certificate to either one or more natural persons (fill in the **Issued to** field) or to the server so that it can be used for automated digital signature tasks in workflow processes (check the **This is a server certificate** box).
4. Click **OK**.

    The **Certificate password** dialog displays.

5. Enter the password you want to assign to the self-signed certificate, then click **OK**.

    > ***Depending on your system's features, you may not be able to choose passwords longer than 7 characters for self-signed certificates. See the Installation manual, "Java Installation" > "Unlimited strength cryptography Java extension".***

    The new certificate now appears in the **Certificates list**: it is now available to sign documents for internal use.

> ***In the "Certificates list", self-signed certificates have the icon, while certificates that have been imported to Gargantua have the icon.***

Assigning a certificate to one or more users

Depending on their assignment, there are two main types of certificates:

- **Server** certificates, used to sign documents automatically as part of Workflow processes;
- Certificates assigned to a user, group or role, used to sign documents one by one on the Web Client.

To assign a certificate to the server, proceed as follows:

1. Check the corresponding Server box in the **Certificates list**.

    A confirmation message displays.

2. Click **Yes**.

    A dialog displays.

3. Enter the password for the certificate, then click **OK**.

    The assignment has been performed: it is now possible to set up digital signature workflow tasks using this certificate.

To assign a certificate to a user, group or role, proceed as follows:

1. In the **Certificates list**, click the corresponding  icon.

   A dialog displays.

2. In the **Name** field, enter the first letters of the appropriate user, group or role name.
3. In the drop-down list, double-click the item of your choice.

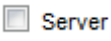
   The assignment has been made: the corresponding users will now be able to select the certificate from the **User certificates** list in Gargantua Web Client.

Assigning a certificate to one or more users

Depending on their assignment, there are two main types of certificates:

- **Server** certificates, used to sign documents automatically as part of Workflow processes;
- Certificates assigned to a user, group or role, used to sign documents one by one on the Web Client.

To assign a certificate to the server, proceed as follows:

1. Check the corresponding 

box in the **Certificates list**.

   A confirmation message displays.

2. Click **Yes**.

   A dialog displays.

3. Enter the password for the certificate, then click **OK**.

   The assignment has been performed: it is now possible to set up digital signature workflow tasks using this certificate.

To assign a certificate to a user, group or role, proceed as follows:

1. In the **Certificates list**, click the corresponding  icon.

   A dialog displays.

2. In the **Name** field, enter the first letters of the appropriate user, group or role name.
3. In the drop-down list, double-click the item of your choice.

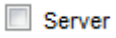
   The assignment has been made: the corresponding users will now be able to select the certificate from the **User certificates** list in Gargantua Web Client.

Assigning a certificate to one or more users

Depending on their assignment, there are two main types of certificates:

- **Server** certificates, used to sign documents automatically as part of Workflow processes;
- Certificates assigned to a user, group or role, used to sign documents one by one on the Web Client.

To assign a certificate to the server, proceed as follows:

1. Check the corresponding  box in the **Certificates list**.

   A confirmation message displays.

2. Click **Yes**.

   A dialog displays.

3. Enter the password for the certificate, then click **OK**.

   The assignment has been performed: it is now possible to set up digital signature workflow tasks using this certificate.

To assign a certificate to a user, group or role, proceed as follows:

1. In the **Certificates list**, click the corresponding  icon.

   A dialog displays.

2. In the **Name** field, enter the first letters of the appropriate user, group or role name.
3. In the drop-down list, double-click the item of your choice.

   The assignment has been made: the corresponding users will now be able to select the certificate from the **User certificates** list in Gargantua Web Client.

Viewing the information in a certificate

To view the information in a certificate, proceed as follows:

1. Select the certificate in the **Certificates list**.
2. Click the **Show details** button in the bottom left corner of the right pane.

   The information in the certificate displays in read-only mode. Besides, some restricted-access information is replaced with the word **Unknown**.

3. To view all the restricted-access information in the certificate, click the **Authenticate** button, and enter the certificate password.

   The restricted-access information is now displayed.

4. When you are done, click **OK** to close the dialog.

Exporting a certificate

Gargantua Administration Tool allows you to export certificates from the server to your hard drive or to a USB eToken, whether the certificates were originally imported or generated using the internal CA.

To export a certificate to your hard drive, proceed as follows:

1. In the bottom right corner of the **Manage certificates** screen, click the **Export to disk** button.

   The file explorer displays.

2. Browse to the local folder where you want to export the certificate, and click **Save**.

   A confirmation message displays.

3. Click **OK**.

   The certificate has been successfully exported to your hard drive.

To export a certificate to a USB eToken, proceed as follows:

1. Make sure that the eToken is connected to your workstation.
2. In the bottom right corner of the **Manage certificates** screen, click the ▼ arrow on the left of the **Export to disk** button.
3. In the list that displays, select the **Export to USB eToken** option.

   A dialog displays.

4. Enter the password for the eToken, then click **OK**.

   A dialog displays.

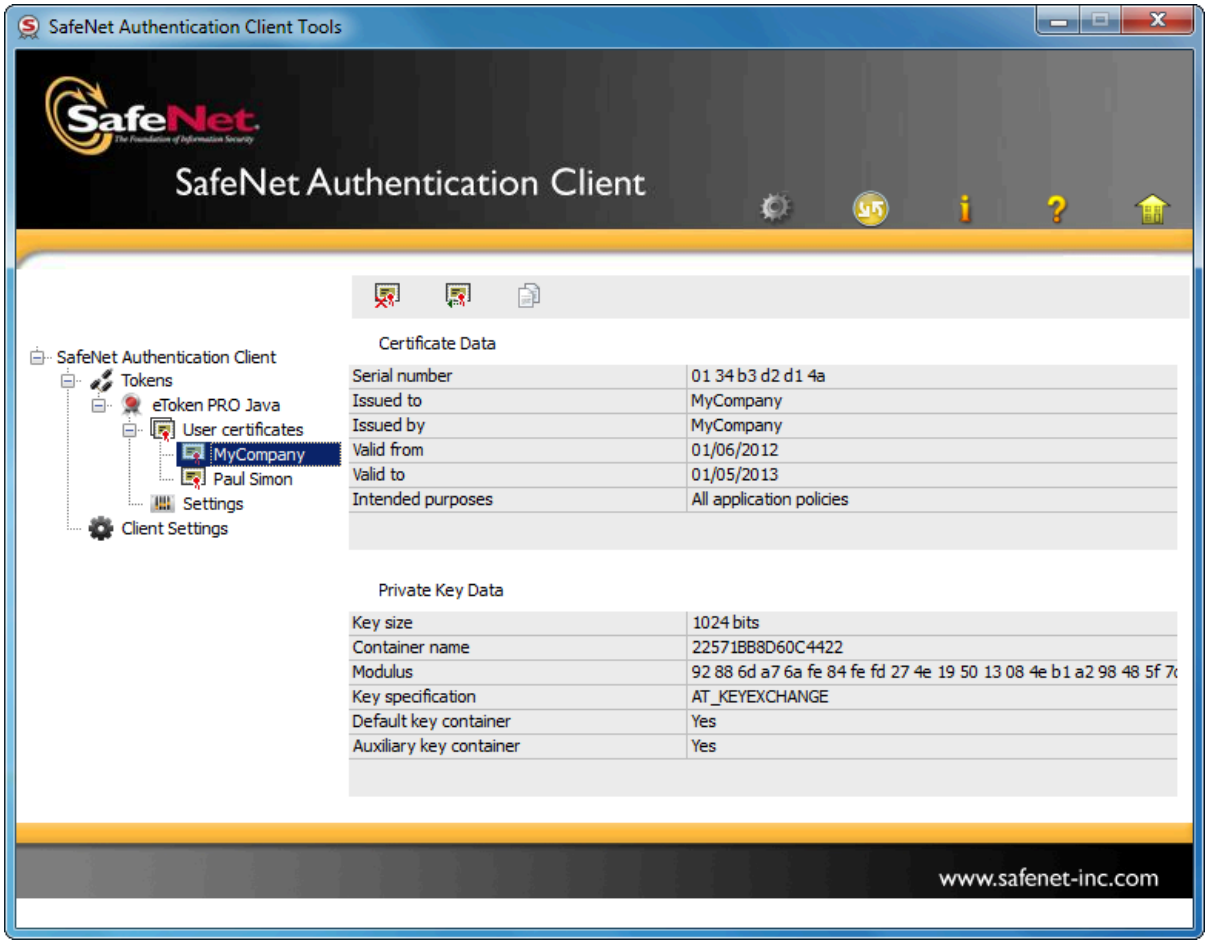
5. Enter the password for the certificate you want to export, then click **OK**.

   A confirmation message displays.

6. Click **OK**.

   The certificate has been exported to the eToken.

   If you explore the contents of the USB key using SafeNet Authentication Client, you can now see it, either under the **User certificates** heading if the certificate was issued by a trusted CA, or under the **AC certificates** heading if the certificate is self-signed:



Deleting a certificate stored on the server

To delete a certificate stored on the server, proceed as follows:

1. Select the certificate in the **Certificates list**.
2. In the bottom left corner of the **Manage certificates** screen, click the **Delete** button.

   A warning message displays.

3. Click **Yes**.

   The certificate has been successfully deleted: it does not display in the **Certificates list** anymore.

> ***Web Client users who have access to the "Settings" link can also delete certificate files from the server (Settings > Signature and certificate settings > User certificate settings), provided they have uploaded the files in the first place, and those have not been reassigned to other users by an administrator (see Importing a certificate stored locally).***