

# D2S SIGN&VALIDATE Version 3.2

## MANUAL



No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, photocopying, recording, or otherwise, without prior written permission of the publisher.

© Copyright 2003 D Soft nv  
Boelenaar 1, 9031 Drongen, Belgium  
E-mail: [info@dsoft.be](mailto:info@dsoft.be)  
Website: [www.dsoft.be](http://www.dsoft.be)  
[www.d2s.org](http://www.d2s.org)  
All Rights Reserved.

---

1. Introduction and installation .....	4
1.1 Introduction .....	4
1.2 Installation .....	4
2. Work area .....	5
2.1 File .....	6
2.2 Signatures .....	6
2.3 View .....	7
2.4 Help .....	7
3. Preferences .....	8
3.1 Certificates .....	8
3.2 Images .....	10
3.3 Visualization .....	11
3.4 Password .....	12
3.5 Reasons .....	13
3.6 Locations .....	14
3.7 CRL/Trust Chain .....	15
3.8 Format .....	16
3.9 File Repository .....	17
4. Signatures .....	18
4.1 Validate .....	18
4.1.1 To verify signature details .....	18
4.1.2 To verify full signature details .....	19
4.2 Sign .....	20
5. Tips and Tricks .....	22

# I Introduction and installation

## I.1 Introduction

The 'D Soft D2S Sign&Validate' application is developed for Win32. Currently an English and Dutch version of the software is available. The D2S products work with any X509 based certificate.

The following platforms and certificates are supported:

- Platforms: Win95 (Service Release 2)  
Win98  
WinNT 4.x and newer  
WinME  
Win2000  
WinXP Home/Professional
- Certificates: All X509 compliant certificates

The D2S products can use certificates stored in:

- Smart cards
- USB tokens
- Microsoft CSP

*Remark: It is recommended that you use the same language for D2S as your operating system.*

*Netscape users should export their certificate and import it in the Windows CSP by using 'Internet Explorer', if they want to use D2S (for more information, see "Tips and Tricks" on page 22).*



## I.2 Installation

An installation programme is included with D2S Sign&Validate. Double-click the application and follow the guidelines on the screen to install the Plug-in.

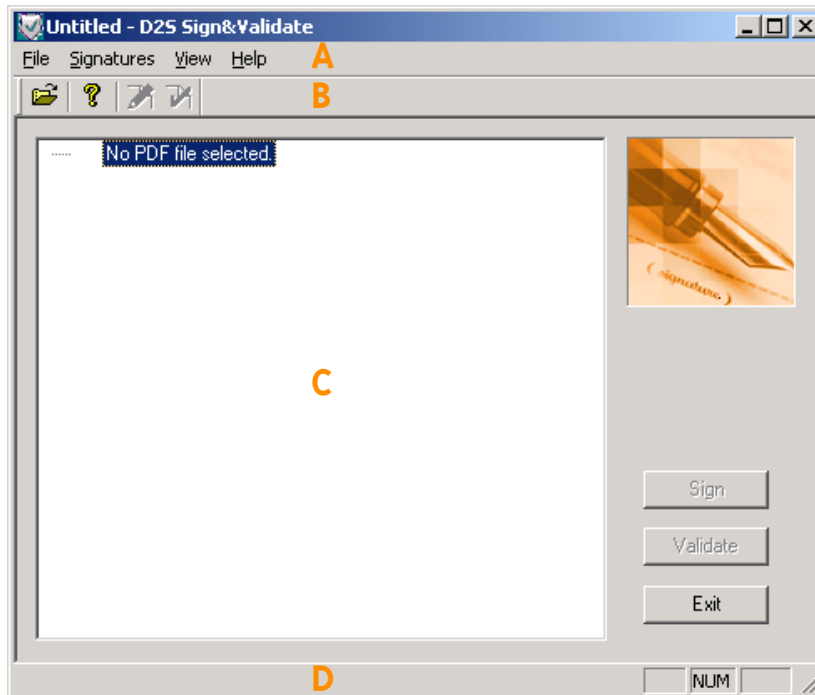
## 2 Work area

To start D2S Sign&Validate:



- double-click the D2S icon on your desktop, or
- choose 'Start > Programs > D Soft > D2S Sign&Validate'.

The following window appears:



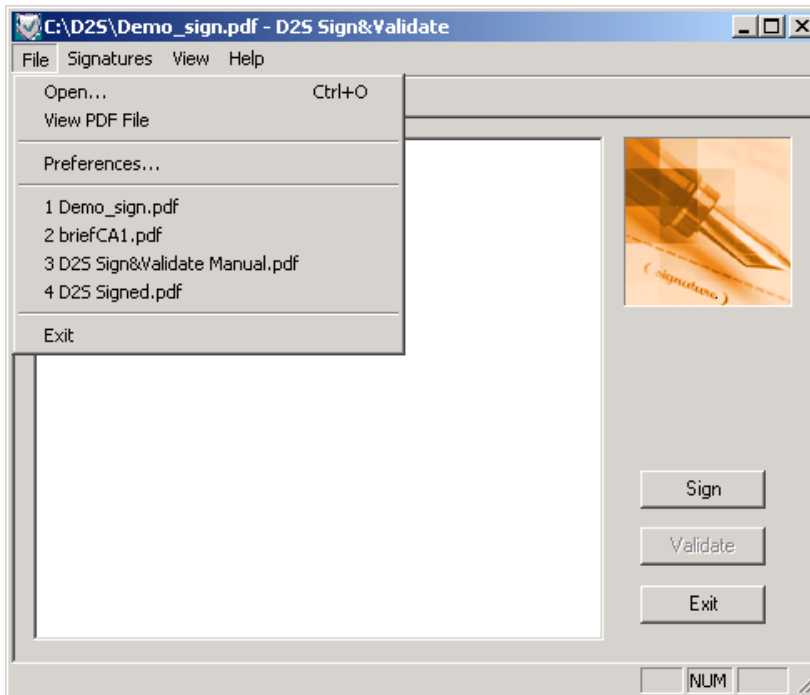
The D2S Sign&Validate work area consists of:


- menu bar (A)
- tool bar (B)
- viewing pane (C)
- status bar (D)

All functions can be executed using the menu bar. The tool bar contains buttons for the most important functions. The signatures present in the current PDF document are shown in the viewing pane.

When you move your mouse pointer over one of the functions of D2S Sign&Validate, the status bar at the bottom of the window shows a short explanation.

## 2.1 File



- Click 'File > Open' to select a PDF document that needs to be signed or validated, or click  from the tool bar.
- Click 'File > View PDF File' to view the PDF document in Acrobat 5.x.
- Choose 'File > Preferences...' to modify your personal settings. D2S Sign&Validate uses a configuration file. This file contains some general settings and your own preferences (see chapter 3).
- Click 'File > Exit' to quit the application or press the 'Exit' button next to the viewing pane.

## 2.2 Signatures



- Validate:

Choose 'Signatures > Validate' from the menu.

You validate a signature to verify that the signed document version has not been altered and to confirm the identity of the signer. You can also use the 'Validate' button next to the viewing pane (for more information see 4.1).

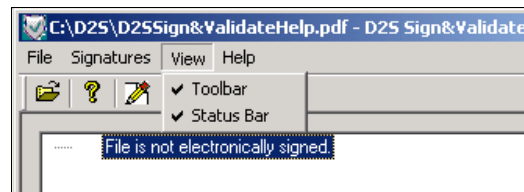


- Sign:

Choose 'Signatures > Sign' to add a signature to the PDF document or click the 'Sign' button next to the viewing pane (for more information see 4.2).

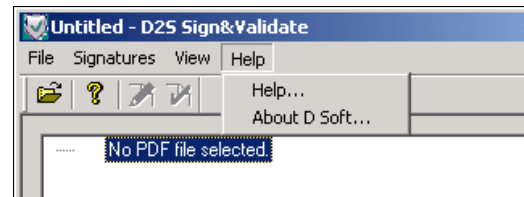
## 2.3 View

- Choose 'View > Toolbar' and/or 'View > Status Bar' to show or hide the tool bar and/or status bar. A check mark appears in the menu next to 'Toolbar' and/or 'Status Bar' if it is currently visible.



## 2.4 Help

- Choose 'Help > Help... ' from the 'Help' context menu, if you need help on using D2S Sign&Validate.
- Choose 'Help > About D Soft... ' for information on D Soft.



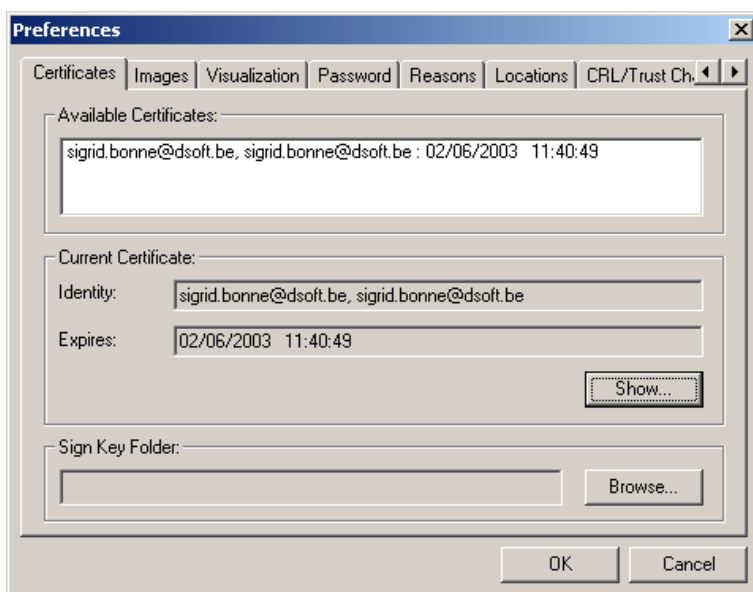
## 3 Preferences

The 'Preferences...' dialog contains several sections to set your personal preferences:

- 'OK': save
- 'Cancel': don't save

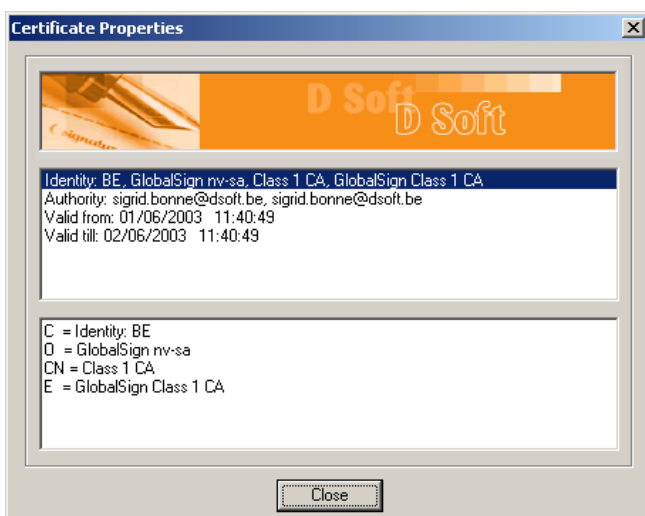
### 3.1 Certificates

Before you can sign a document, you should select your default certificate from the list of available certificates. The certificate you have chosen will be used by D2S Sign&Validate to sign your PDF files.

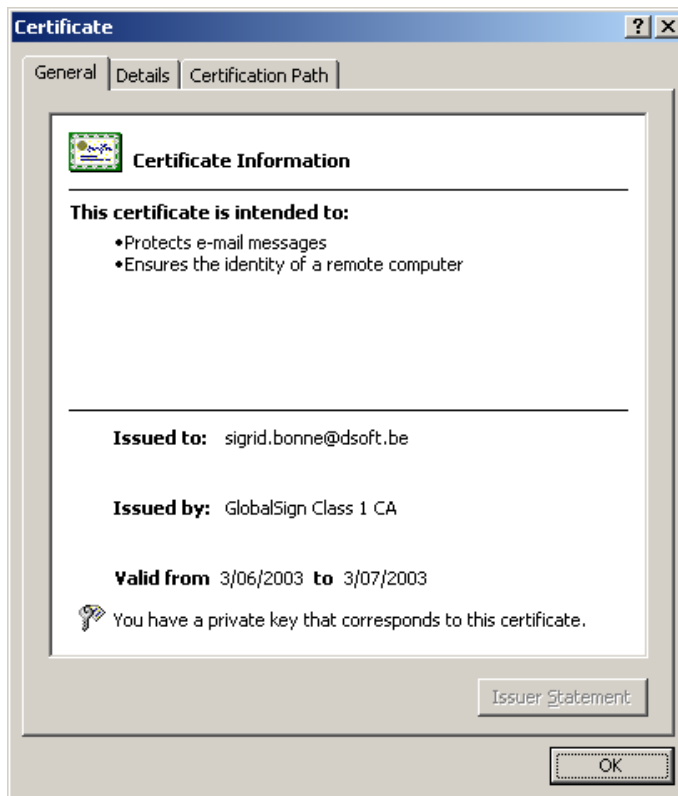


- Press 'Show...' to view all the details of the current certificate. The properties of the certificate are shown in the following screen:

Windows 95



Windows 98/ME/2000/XP/NT



- You can browse for a folder containing the Sign Key file that matches the certificate by clicking the 'Browse...' button. This folder (C:\Program Files\D Soft\D2S\SignKey) has already been created by the application.

There are 3 different types of certificates:

- Class 1: this is a demo certificate.  
There is no identity verification of the applicant.  
This certificate can always be used by D2S Sign&Validate to sign as well as validate.
- Class 2: used for f.e. transactions with low value.  
Limited verification: the applicant needs to send a copy of his identity card.  
D2S Sign&Validate needs a valid Sign Key\* in order to use Class 2 certificates.  
A Sign Key is linked to either the public key of your certificate or to the e-mail address as mentioned in the subject of your certificate.
- Class 3: high guarantee value (covers up to € 37.500)  
Identity-verification of the applicant according to strict rules.  
D2S Sign&Validate needs a valid Sign Key\* in order to use Class 3 certificates.

*Remark: Certificates and Sign Keys are only needed for signing a PDF file. Validation of signatures is always possible.*

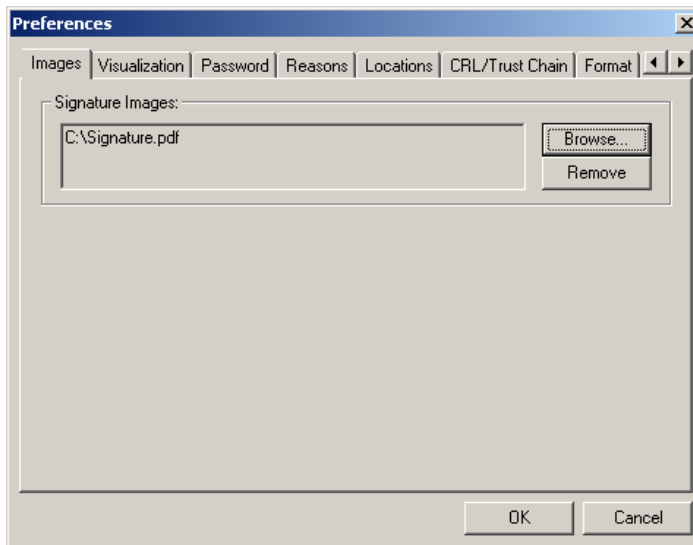
*\* You can request a Sign Key at [www.d2s.org](http://www.d2s.org). A link where you can download your Sign Key will be mailed to you.*

## 3.2 Images

If you want to add an image of your signature to the PDF document when signing, you should configure it in the 'Images' section of the 'Preferences' window.

The image needs to meet the following conditions:

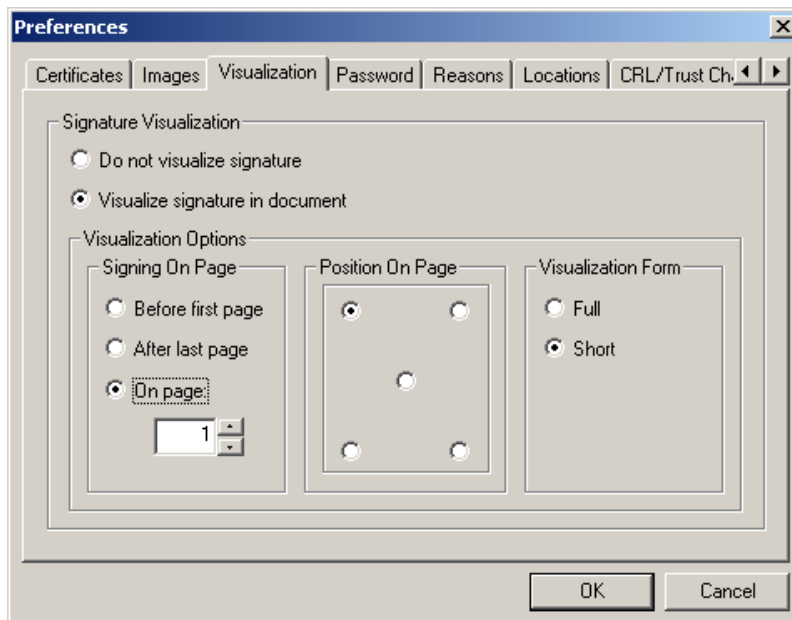
- The selected file must be a PDF document that contains only the image of the signature.
- The PDF document should not be 'cropped'.
- The best results are obtained if the signature is placed on a transparent background.



- Click the 'Browse...' button to select the PDF document containing the image.
- Click the 'Remove' button to remove the image.

### 3.3 Visualization

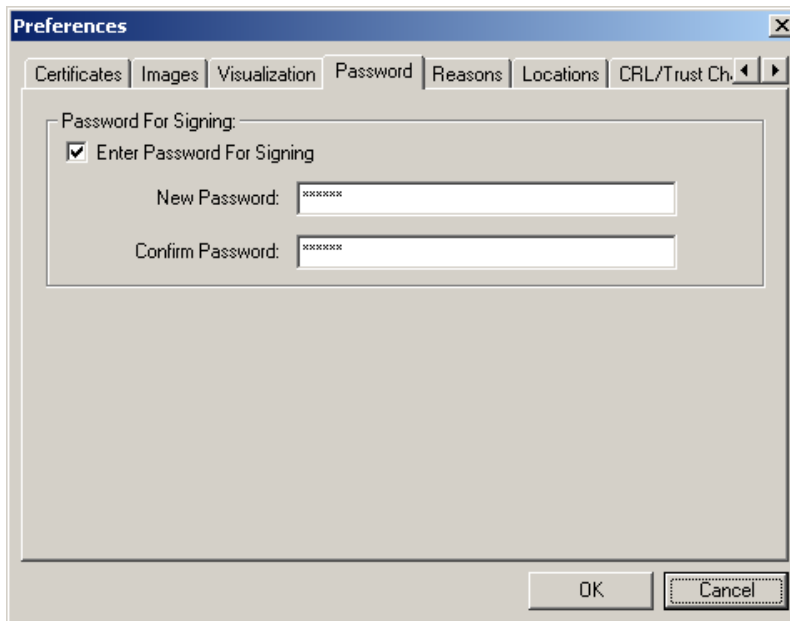
You can specify whether you want to display the signature or not in the 'Visualization' section.



- If you do not wish to see an appearance of the signature displayed on your PDF document, select the 'Do not visualize signature' option. In this case the document is signed, but this will only be visible in the 'Signatures' section of Acrobat 5.x.
- Select 'Visualize signature in document' if you want a physical appearance. Choose one of the following options to position the signature:
  - 'Signing On Page'
    - If you choose 'Before first page' or 'After last page', a blank page with your signature will be added before the first or after the last page of the PDF document.
    - If you choose 'On page', the signature will be placed on the specified page.
  - 'Position On Page'
    - Select where the signature should be positioned on the page.
  - 'Visualization Form'
    - When you choose 'Full', the image of the signature appears together with the date and identity of signing. If no image is configured, signing will default to 'Short'.
    - When you choose 'Short', only the date and identity of signing appear on the PDF document.

### 3.4 Password

You can specify whether a password is required for signing or not, in the 'Password' section of the 'Preferences' window.



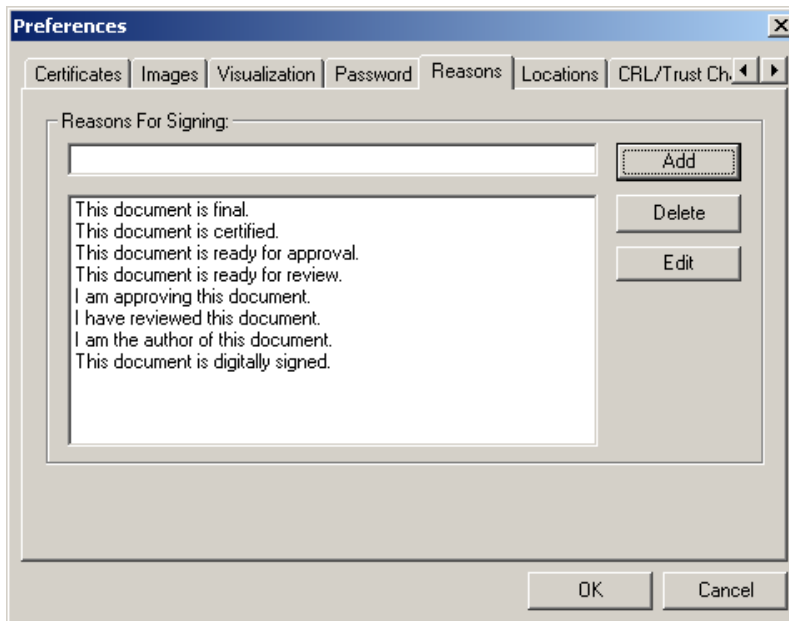
The password and a confirmation are requested. Only digits and standard characters (A - Z, a - z) are allowed.

You are also asked for this password when you want to reset this option to 'no password required'.

*Remark: The password is case-sensitive.*

### 3.5 Reasons

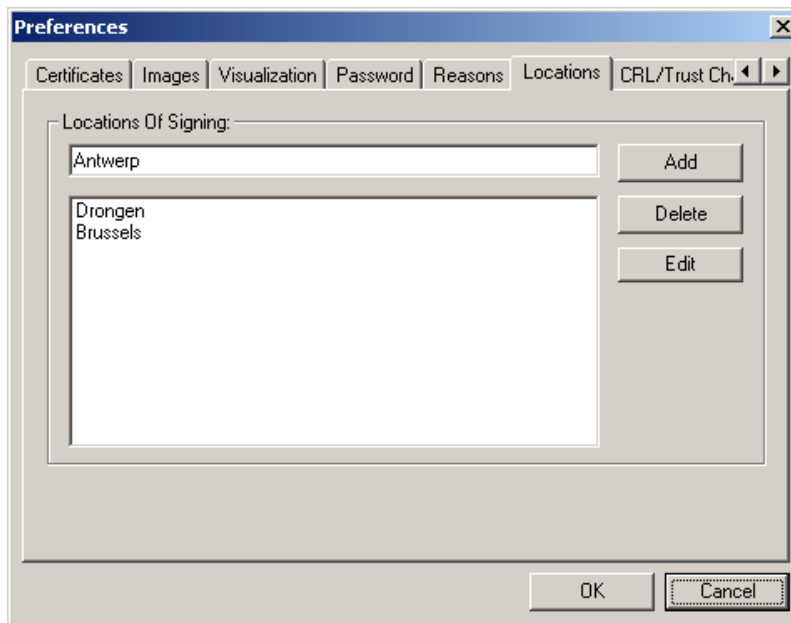
You can add your own reasons and edit or remove existing reasons in the 'Reasons' section of the 'Preferences' window.



- Add your own reason by clicking the 'Add' button.
- Select a predefined reason to delete or edit and press the 'Delete' or 'Edit' button.

### 3.6 Locations

You can add your own locations and edit or remove existing locations in the 'Locations' section of the 'Preferences' window.



- Add your own location by clicking the 'Add' button.
- Select a predefined location to delete or edit and press the 'Delete' or 'Edit' button.

### 3.7 CRL/Trust Chain

You can set additional criteria to define the validity of the certificate in the 'CRL' window. Besides checking the integrity of the signature, the following checks can be performed during the validation of a signature.

The certificate trust chain can be checked.

You have a choice between:

- Check the issuer's integrity of the certificate tree.

You have a choice between:

- a. Using the CA/Root certificates that are included in the signature for checking the trust chain (uncheck the second checkbox).
  - b. Using the CA/Root certificates stored in the Microsoft certificate store when checking the trust chain (check the second checkbox).
- Verify that the signer's certificate is not listed in the CRL and therefore is not revoked.

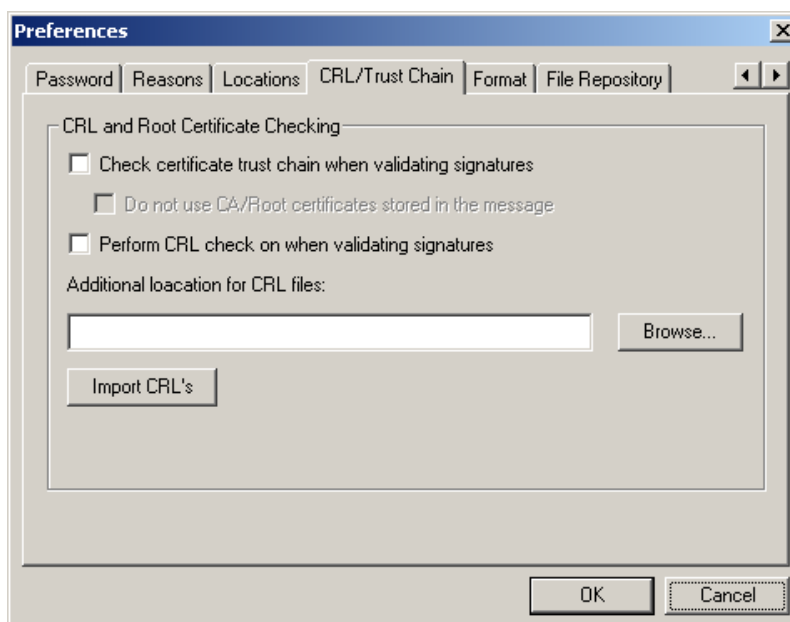
Only the revocation of certificates with a CRL distribution point specified can be checked. If you have an Internet connection, these CRL's will automatically be downloaded and installed on your PC.

Certificates listed on the CRL are revoked and a signature based on such a certificate will be visualised as invalid after validation (f.e. by loss, theft, ...).

If you don't have an Internet connection you can still check the revocation of a certificate by importing these CRL's yourself.

- Additional CRL folder:

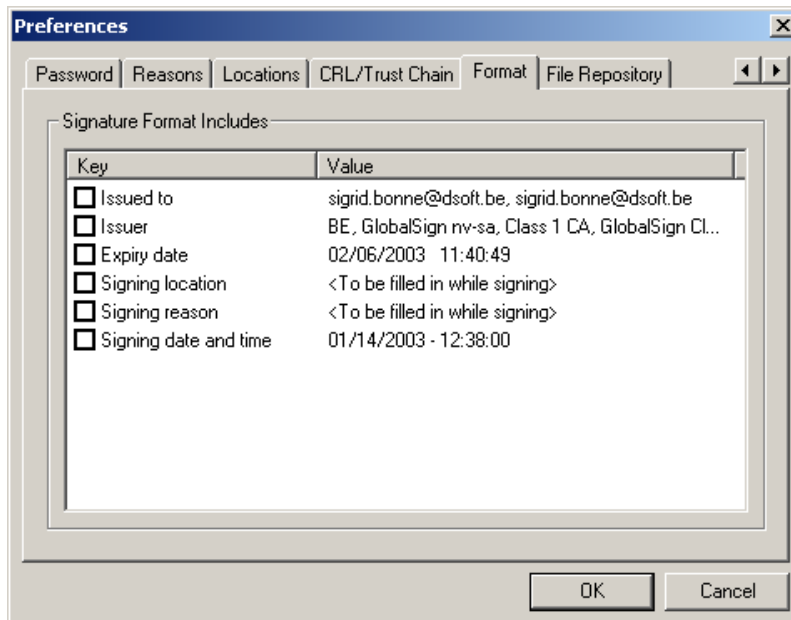
Copy the downloaded CRL on your system. Browse for the location where the imported CRL's are stored and click 'Import CRL's' if you want to use them.



### 3.8 Format

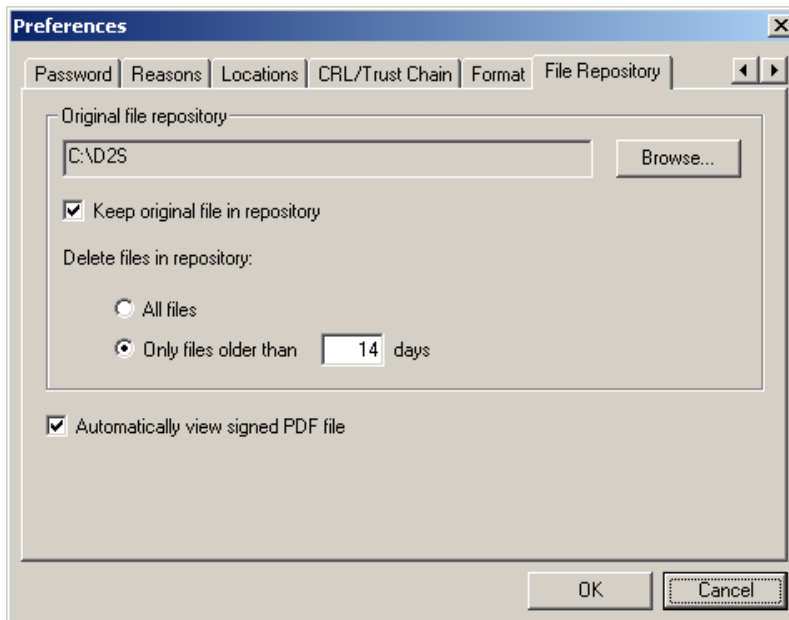
D2S Sign&Validate lets you specify the contents of the signature's text.

- In the 'Signatures Format Includes' field, select the keys that need to be displayed on the PDF document.



### 3.9 File Repository

D2S Sign&Validate lets you specify a 'File Repository' to store a copy of the original PDF document. This can be useful if you want to keep the original version of the PDF you want to sign f.e. as a backup file.



- Browse for a folder to store the original PDF document, by clicking the 'Browse...' button.
- Select 'Keep original file in repository' to keep a copy of the original file in the specified folder.
- Choose 'All files' if the original PDF files present in the folder should be deleted when starting the application. D2S Sign&Validate only removes the PDF documents in this folder.
- By selecting 'Only files older than ...' and entering a number of days, the application removes all PDF documents stored in the specified folder older than the specified number of days (when starting up the application).
- Check 'Automatically view signed PDF file' to automatically open the PDF document in Acrobat 5.x after signing.


## 4 Signatures






You can view the properties of a signature in the 'D2S Sign&Validate' window.

### 4.1 Validate


You should validate a signature to verify that the signed document version has not been altered and to confirm the identity of the signer.

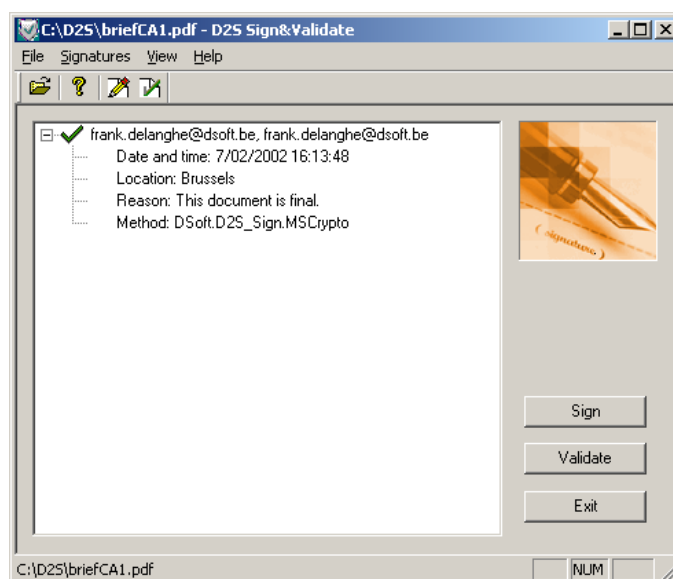
When you add a signature to a document, the information that uniquely identifies you as signer, is added. When you validate, this information is checked.

- Choose 'Signatures > Validate' from the context menu, click the 'Validate' button next to the document pane, or click .

Validation status	Icon in palette
Signed, but not validated.	
Valid, but identity of signer could not be validated. CRL and/or certificate chain checking is asked but not possible.	
Valid and identity of signer is valid. CRL and/or certificate chain checking succeeded when asked.	
Invalid. CRL and/or certificate chain checking failed when asked.	
Document altered after signing.	

#### 4.1.1 To verify signature details

- Click  next to the signature you want to view the properties of. The properties appear in the 'D2S Sign&Validate' window.



- 'Name': distinguished name of the certificate holder.
- 'Date and time': date and hour on which the signature was applied.
- 'Location': signing location (optional).
- 'Reason': signing reason (optional).

#### 4.1.2 To verify full signature details

- Select and right-click the validated signature in the 'D2S Sign&Validate' window. The 'Signature properties' window appears.




#### Validity

- 'Signature valid/invalid/unknown': indicates whether or not the file has been tampered with.
- 'Check on certificate chain': ok, not possible, not asked, failed. Not possible indicates that the CA and/or root certificates were not included in the signature. Not asked indicates that no check was performed (see "CRL/Trust Chain" on page 15).
- 'Check on CRL validity': ok, not possible, not asked, failed. Not possible indicates that no CRL is present on the system. Not asked indicates that no check was performed (see "CRL/Trust Chain" on page 15).
- 'Check on certificate versus CRL': ok, not possible, not asked, failed. Not possible indicates that no valid CRL was found on the system. Not asked indicates that no check was performed (see "CRL/Trust Chain" on page 15). Ok indicates that the certificate does not appear on any valid CRL.
- 'Signing time within cert. validity period': ok or failed. Indicates whether or not the signature was created within the validity period of the signer's certificate.

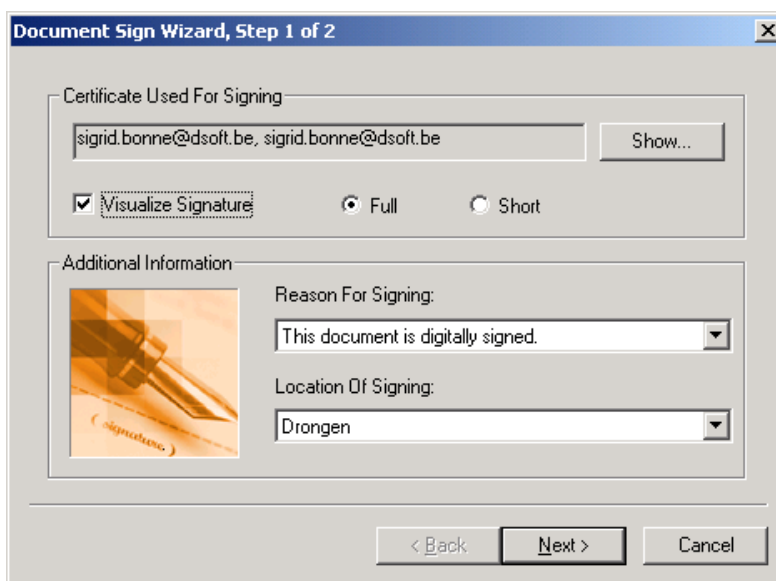
### Properties

- Signed by: distinguished name of the signer.
- Date: date and hour on which the signature was applied.
- Reason: signing reason
- Location: signing location
- Certificate details: the issuing Certification Authority, expiry date and issuing date.

## 4.2 Sign

- Choose 'Signatures > Sign' from the menu list, click 'Sign' next to the document pane, or click .

The following window appears:



### Certificate Used For Signing

- Press the 'Show...' button to view the properties of the certificate to be used.

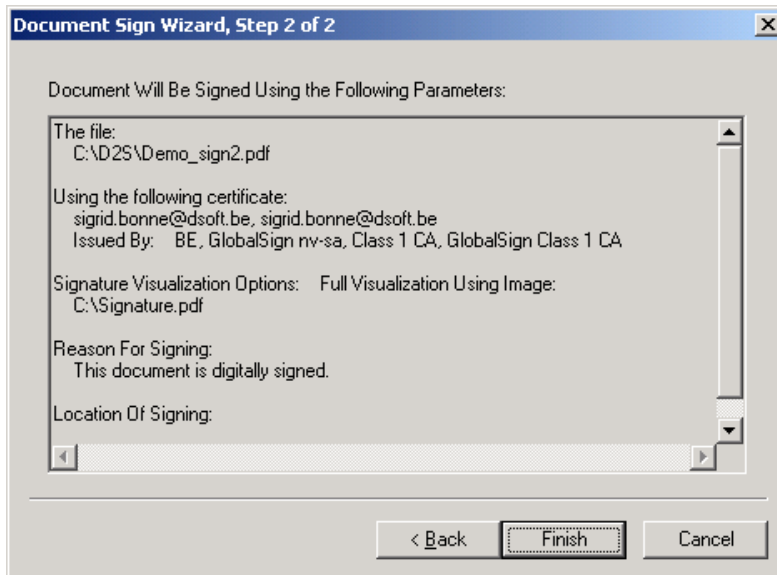
### Visualisation

You can visualise the signature on the PDF document.

- When you choose 'Full', the image of the signature appears together with the date and identity of signing on the PDF document. This option is only available if an image of the signature is configured (see 3.2).
- When you choose 'Short', only the date and identity of signing appear on the PDF document.
- When you choose no visualisation, the document is signed, but this is only visible in the 'Show signatures' option in Acrobat 5.x (not in the Reader).

### Additional Information

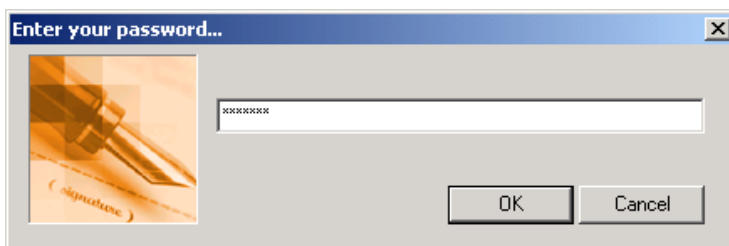
- Choose the reason and location for signing, if needed. The list of available reasons and locations can be modified in the preferences (see 3.5 and 3.6).
- Click the 'Next' button and the 'Step 2 of the Document Sign Wizard' window appears.



This window shows a list of the previously defined settings. The PDF document will be signed using these parameters.

- Click 'Back' if you still want to modify a parameter.
- Click the 'Finish' button, the 'Save As' dialogue appears only the first time a document is signed.

You are asked for a password, if one is required for signing (see 3.4).



- Enter your password and click 'OK'.
- Enter a filename, specify a location and click 'Save'. You can name the PDF file only the first time you sign it. You cannot use the 'Save As' command on a signed document. The new signature appears as the last item in the viewing pane, with an icon signifying that it is valid.

## 5 Tips and Tricks

- Netscape users should export their certificate and import it in the Windows CSP by using 'Internet Explorer', if they want to use D2S.

To export your certificate using Netscape:

- Open the 'Security Info' window by clicking the 'Lock' icon in the tool bar. Select 'Certificates', then 'Yours'.
- Select the certificate you want to export and click 'Export'.
- You are asked for a password to protect the data and a location to store the exported certificate.

To import your certificate using Internet Explorer:

- Select 'Internet Options...' from the 'Tools' menu of Internet Explorer.
- Click on the 'Certificates...' button in the 'Content' tab.
- Follow the instructions on the screen after clicking the 'Import ...' button.
- You are asked for the location of the file you generated in Netscape.

After completing these steps your certificate can be used by the 'D2S Sign&Validate' (refer to 3 Preferences).