

D2S SIGN&VALIDATE

Versie 3.2

H A N D L E I D I N G



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@d2s.org
Website: www.dsoft.be
www.d2s.org
All Rights Reserved.

| | |
|--|----|
| 1. Inleiding en installatie | 4 |
| 1.1 Inleiding | 4 |
| 1.2 Installatie | 4 |
| 2. Werkgebied | 5 |
| 2.1 Bestand | 6 |
| 2.2 Handtekeningen | 6 |
| 2.3 Beeld | 7 |
| 2.4 Help | 7 |
| 3. Instellingen | 8 |
| 3.1 Certificaten | 8 |
| 3.2 Figuren | 10 |
| 3.3 Afbeelding | 11 |
| 3.4 Paswoord | 12 |
| 3.5 Redenen | 13 |
| 3.6 Locaties | 14 |
| 3.7 CRL/Cert. Keten | 15 |
| 3.8 Formaat | 16 |
| 3.9 Originelen | 17 |
| 4. Handtekeningen | 18 |
| 4.1 Valideren | 18 |
| 4.1.1 Nakijken van de eigenschappen van een handtekening | 18 |
| 4.1.2 Verifiëren van de volledige handtekeningdetails | 19 |
| 4.2 Ondertekenen | 20 |
| 5. Tips & Tricks | 22 |

I Inleiding en installatie

I.1 Inleiding

De 'D Soft D2S Sign&Validate' applicatie is ontwikkeld voor Win32 systemen. Momenteel is zowel een nederlandse als een engelse versie van de software beschikbaar.

D2S Sign&Validate werkt met alle X509 gebaseerde certificaten.

De volgende platformen en certificaten worden ondersteund:

- Platformen: Win95 (Service Release 2)
Win98
WinME
WinNT 4.x of recenter
Win2000
WinXP Home/Professional
- Certificaten: Alle certificaten conform de X509 standaard

D2S gebruikt certificaten aanwezig in:

- Smart cards
- USB tokens
- Microsoft CSP

Opm.: Het is aan te raden dat u voor D2S dezelfde taal kiest als die van uw operating system.

Netscape gebruikers moeten hun certificaat exporteren en importeren in de Windows CSP via Internet Explorer (voor meer informatie, zie hoofdstuk 5).



I.2 Installatie

Er is een installatieprogramma ontwikkeld voor D2S Sign&Validate. Dubbelklik op deze applicatie en volg de richtlijnen op het scherm om de plug-in te installeren.

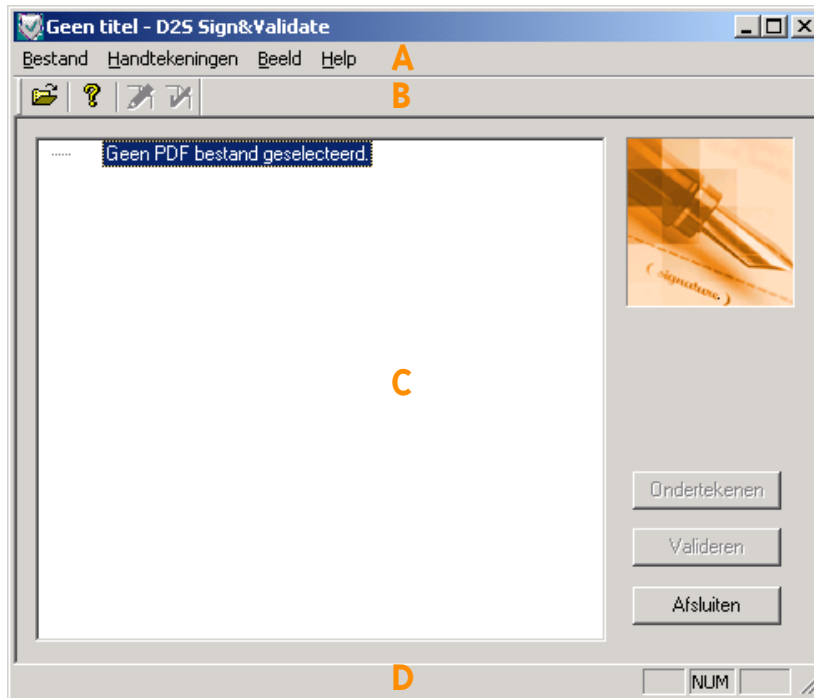
2 Werkgebied



U kunt de applicatie opstarten door:

- op het icoon op uw desktop te dubbelklikken, of
- uit het 'Startmenu > Programma's > D Soft > D2S Sign&Validate' te kiezen.

Het volgende venster verschijnt:



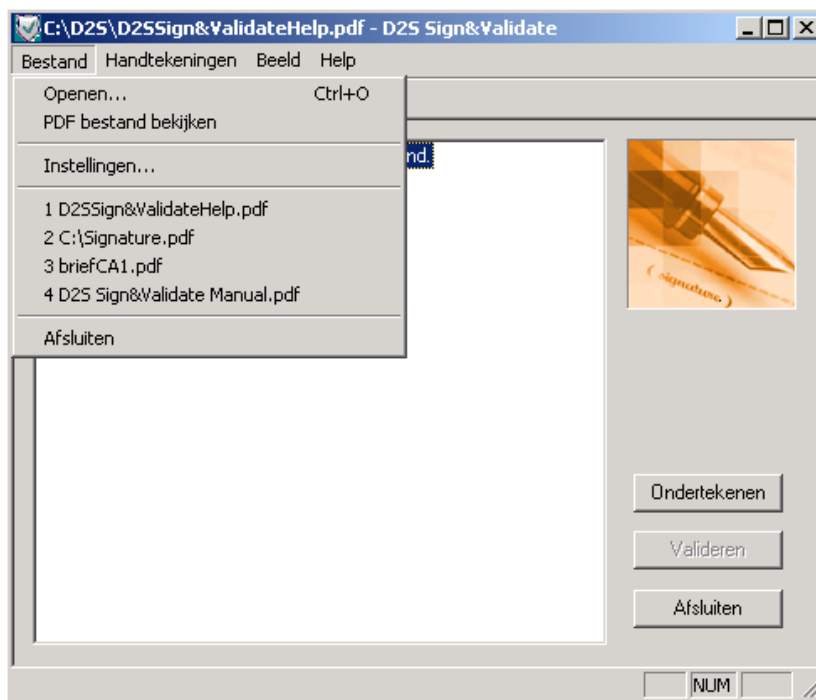
Het startscherm van D2S Sign&Validate bestaat uit verschillende delen:


- menubalk (A)
- werkbalk (B)
- documentvenster (C)
- statusbalk (D)

Alle handelingen kunnen via de menubalk uitgevoerd worden. Voor de belangrijkste zijn knoppen op de werkbalk voorzien. In het documentvenster worden de handtekeningen aanwezig in het geopend PDF document getoond.

Als u met de muis over één van de functies van D2S Sign&Validate beweegt, dan verschijnt een korte uitleg in de statusbalk onderaan.

2.1 Bestand



- Klik op 'Bestand > Openen...' om het PDF document te openen dat ondertekend of gevalideerd moet worden, of klik op  in de werkbalk.
- Klik op 'Bestand > PDF bestand bekijken' om een PDF document in Acrobat te bekijken
- Kies 'Bestand > Instellingen...' om uw persoonlijke instellingen te wijzigen. D2S Sign&Validate gebruikt een configuratiebestand dat naast enkele algemene ook uw persoonlijke instellingen bevat (zie hoofdstuk 3).
- Klik op 'Bestand > Afsluiten' om de applicatie te sluiten of klik op 'Afsluiten' naast het documentvenster.

2.2 Handtekeningen

-  • Valideren:

Kies 'Handtekeningen > Valideren' uit de menubalk.

Door een handtekening te valideren controleer je dat het ondertekende document niet is gewijzigd na ondertekening, ook de identiteit van de ondertekenaar wordt bevestigd. U kunt ook de 'Valideren' knop gebruiken naast het document venster (voor meer informatie, zie 4.1).



-  • Ondertekenen:

Kies 'Handtekeningen > Ondertekenen' om een handtekening aan het PDF document toe te voegen. U kunt ook de 'Ondertekenen' knop gebruiken naast het document venster (voor meer informatie, zie 4.2).

2.3 Beeld

- Kies 'Beeld > Werkbalk' en/of 'Beeld > Statusbalk' om de werkbalk en/of statusbalk weer te geven of te verbergen. Een vinkje verschijnt in het menu naast 'Werkbalk' en/of 'Statusbalk' als deze zichtbaar is.



2.4 Help

- Kies 'Help > Help...'' als u hulp nodig hebt over het gebruik van D2S Sign&Validate.
- Kies 'Help > Info over D Soft...'' voor informatie over D Soft.



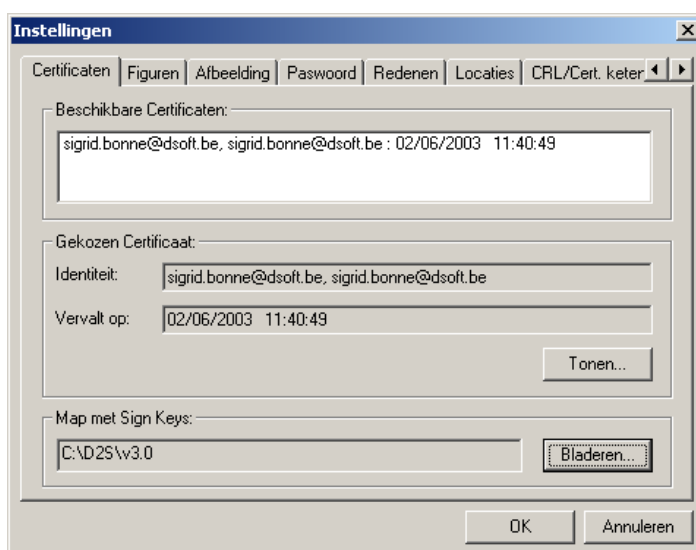
3 Instellingen

Het 'Instellingen' scherm bevat een aantal secties waarin uw persoonlijke voorkeuren kunnen ingegeven worden:

- 'OK': bewaren
- 'Annuleren': niet bewaren

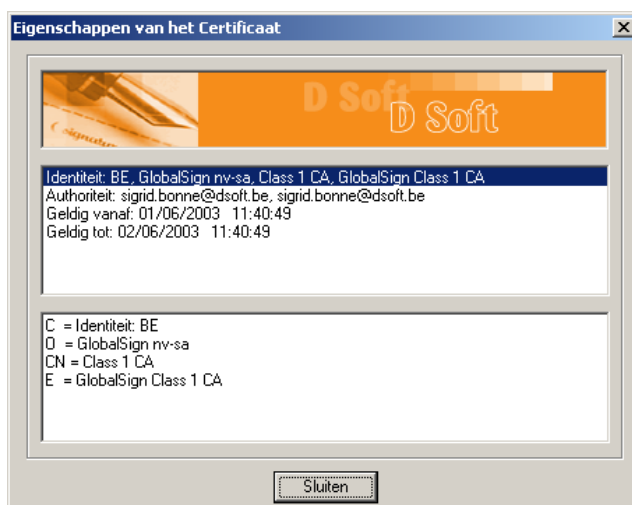
3.1 Certificaten

Vooraleer een document kan ondertekend worden, moet u een 'huidig' certificaat kiezen uit de lijst met beschikbare certificaten. Dit gekozen certificaat zal gebruikt worden bij het ondertekenen van een document. Dit doet u door een certificaat aan te klikken in de lijst. Enkele gegevens verschijnen dan in 'Gekozen Certificaat'.

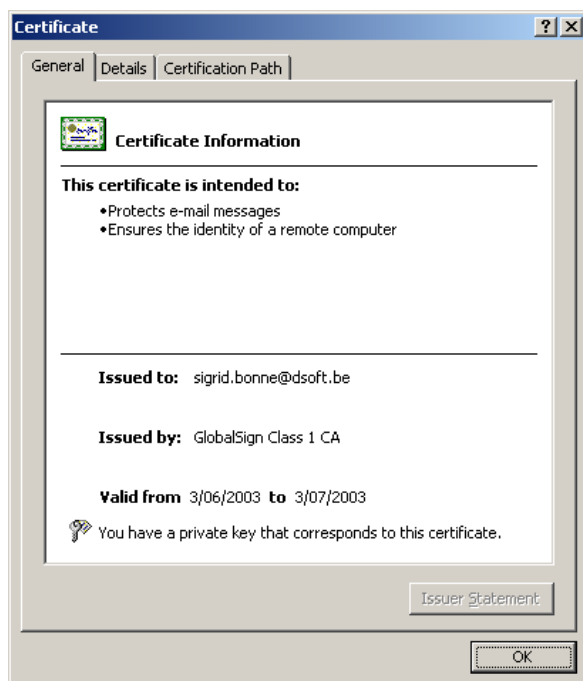


- De 'Tonen...' knop geeft steeds alle eigenschappen weer van het gekozen certificaat.

Windows 95



Windows 98/ME/2000/XP/NT



- Klik op 'Bladeren...' om de folder met de bijhorende Sign Key te selecteren. D2S Sign&Validate creëert automatisch een folder voor Sign keys (C:\Program Files\D Soft\D2S\SignKey).

Er zijn 3 verschillende soorten certificaten:

- Class 1: dit is een demo certificaat.
Er is geen enkele verificatie van de identiteit van de aanvrager. Dit certificaat kan altijd door D2S Sign&Validate gebruikt worden voor valideren en ondertekenen.
- Class 2: bedoeld voor bijvoorbeeld transacties met geringe waarde.
Bepaalde verificatie: de aanvrager dient een kopie van een identiteitsbewijs op te sturen.
D2S Sign&Validate heeft een geldige Sign Key nodig om Class 2 certificaten te kunnen gebruiken. Een Sign Key* kan verbonden zijn aan de 'Public-key' of aan het e-mail adres van uw certificaat.
- Class 3: hoge garantiewaarde (dekking tot € 37.500).
Identiteitsverificatie volgens strikte regels met een fysieke vaststelling van de identiteit van de aanvrager (voor lokale officiële aangestelde autoriteit, bv Stafhouder, Kamer van Koophandel).
D2S Sign&Validate heeft een geldige Sign Key* nodig om Class 3 certificaten te kunnen gebruiken.

Opm.: Certificaten en Sign Keys zijn enkel nodig bij het ondertekenen van een PDF document. Om een handtekening te valideren hebt u geen certificaat of Sign Key nodig.

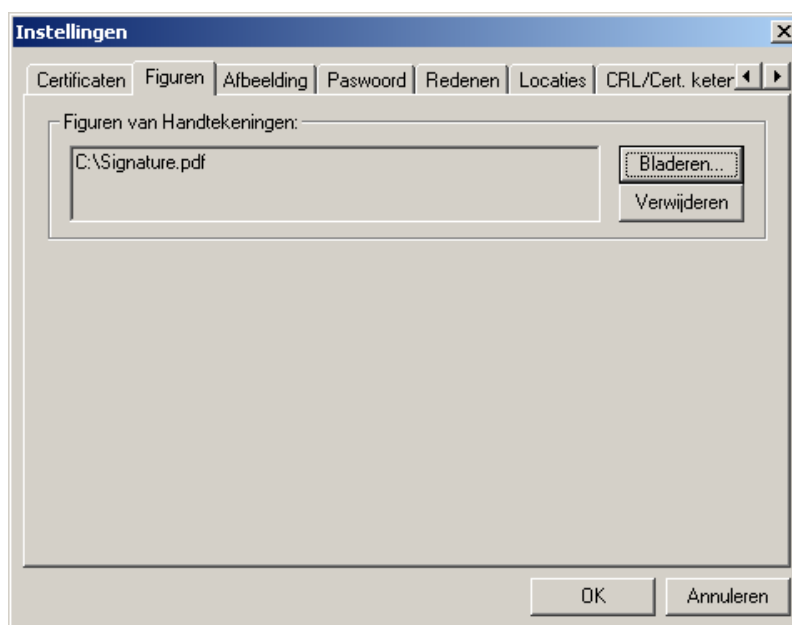
* Een Sign Key kunt u verkrijgen op www.d2s.org. Via e-mail wordt een link toegestuurd waar u de Sign Key kunt downloaden.

3.2 Figuren

Indien een afbeelding van uw handtekening op het PDF document geplaatst moet bij de ondertekening ervan, moet deze geconfigureerd worden in de 'Figuren' sectie van het 'Instellingen' venster.

De gekozen afbeelding moet aan volgende voorwaarden voldoen:

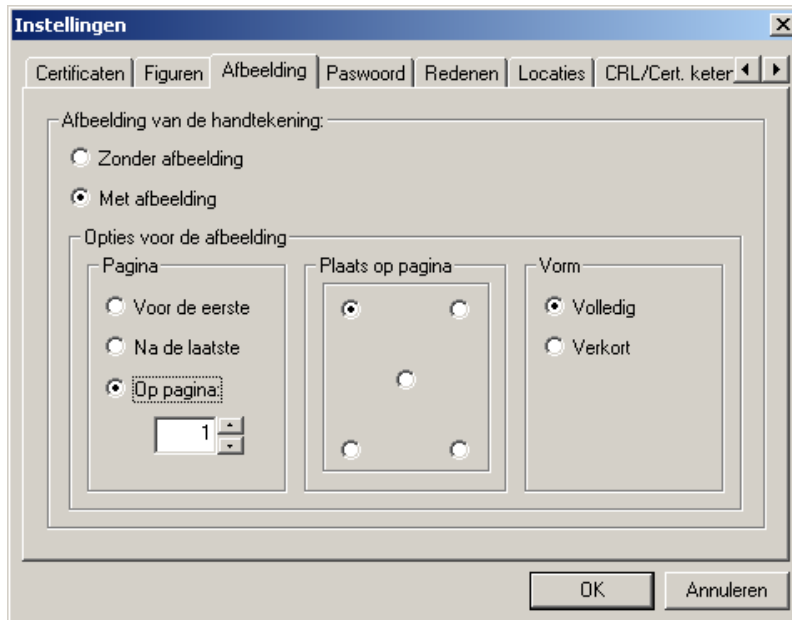
- Het geselecteerde bestand moet een PDF document zijn dat enkel de afbeelding van de handtekening bevat.
- Het PDF bestand mag niet 'bijgesneden' zijn.
- Het beste resultaat wordt verkregen als de handtekening op een transparante achtergrond geplaatst is.



- Klik op 'Bladeren...' om het PDF document met de handtekening te selecteren.
- Klik op 'Verwijderen' om een afbeelding te verwijderen.

3.3 Afbeelding

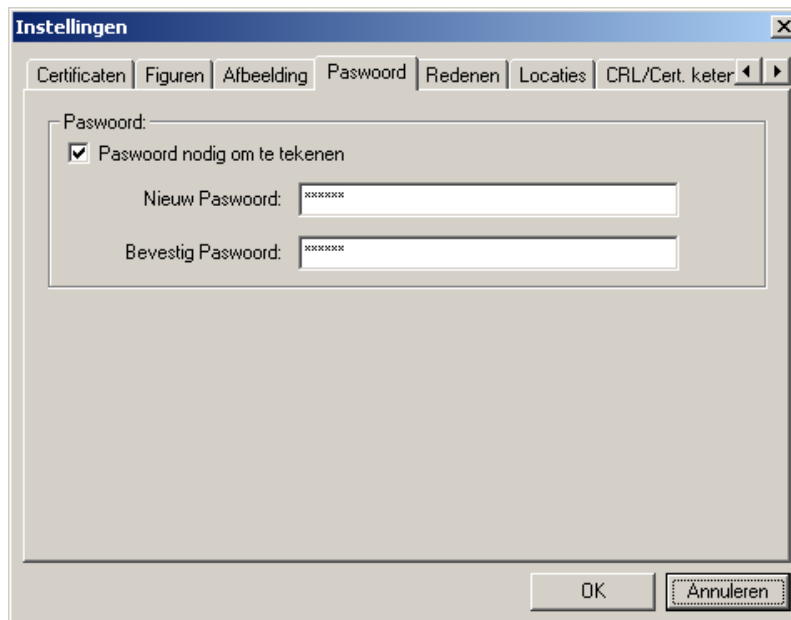
U kunt in 'Afbeelding' sectie bepalen of een afbeelding van de handtekening al of niet zichtbaar is in het PDF document.



- Indien u geen afbeelding van de handtekening in een PDF document wenst, selecteer dan de 'Zonder afbeelding' optie. In dit geval zal het document getekend zijn, maar de handtekening zal enkel zichtbaar zijn in de 'Handtekeningen' sectie van Acrobat (Reader).
- Selecteer 'Met afbeelding' indien u een afbeelding van de handtekening wenst in het PDF document. Kies uit één van de volgende opties om de handtekening te positioneren:
 - 'Pagina'
 - Als u 'Voor de eerste' of 'Na de laatste' kiest, dan zal vooraan respectievelijk achteraan een blanco pagina met uw handtekening aan het PDF document toegevoegd worden.
 - Als u 'Op pagina' kiest, dan wordt de handtekening op de door u ingegeven pagina geplaatst.
 - 'Plaats op pagina'
 - Selecteer waar de handtekening moet geplaatst worden op het PDF document.
 - 'Vorm'
 - Als u 'Volledig' kiest, dan verschijnt naast een afbeelding van de handtekening ook de datum en identiteit van het ondertekenen op het PDF document. Deze optie is enkel beschikbaar als een afbeelding van de handtekening geconfigureerd is.
 - Als u kiest voor 'Verkort' zullen enkel de velden aangeklikt onder de 'Formaat'-tab verschijnen op het PDF document.

3.4 Paswoord

In de 'Paswoord' sectie van het 'Instellingen' venster kunt u aangeven of een paswoord al dan niet vereist is voor het ondertekenen van een document.

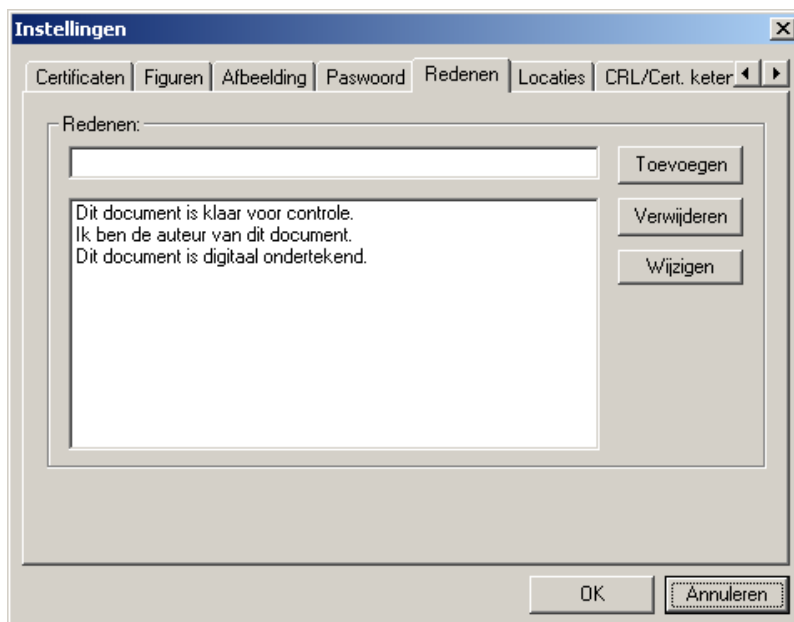


Bij het ingeven van het paswoord en de verificatie ervan zijn enkel cijfers en normale tekens (A - Z, a - z) toegelaten. Dit paswoord wordt ook gevraagd bij het terugzetten van deze optie naar 'geen paswoord nodig'.

Opm.: Het paswoord is case-sensitive.

3.5 Redenen

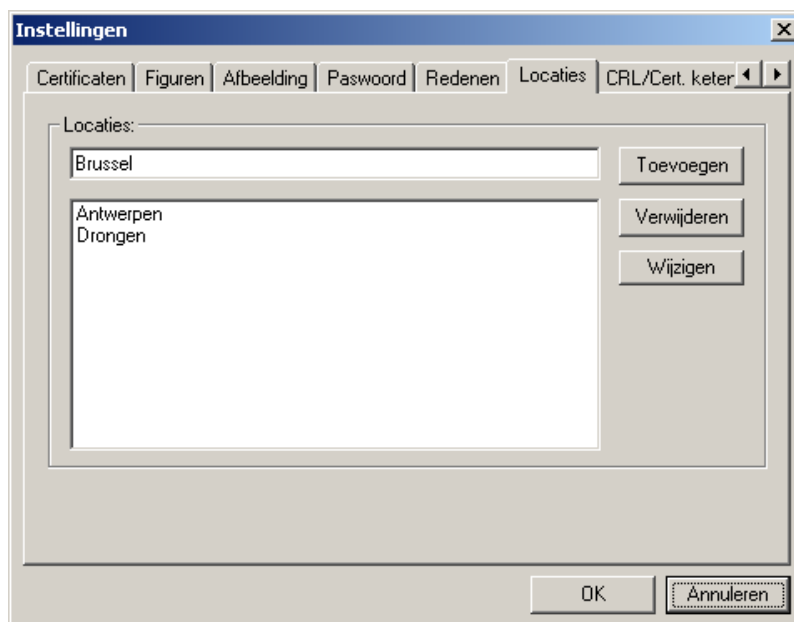
U kunt in de 'Redenen' sectie van het 'Instellingen' venster uw eigen reden voor ondertekening toevoegen en reeds bestaande wijzigen of verwijderen.



- Klik op 'Toevoegen' om een reden aan de lijst toe te voegen.
- Selecteer een reeds gedefinieerde reden voor wijziging of verwijdering en druk op de gewenste knop.

3.6 Locaties

U kunt in de 'Locaties' sectie van het 'Instellingen' venster uw eigen locaties toevoegen en reeds bestaande wijzigen of verwijderen.



- Klik op 'Toevoegen' om een locatie aan de lijst toe te voegen.
- Selecteer een reeds gedefinieerde locatie voor wijziging of verwijdering en druk op de gewenste knop.

3.7 CRL/Cert. Keten

U kunt criteria die de geldigheid van het certificaat bepalen instellen via het 'CRL' venster. Naast de controle op de integriteit van de handtekening kunnen volgende bijkomende controles uitgevoerd worden tijdens het valideren van een handtekening:

- Controle op de integriteit van de boom van uitgevers van het certificaat van de ondertekenaar (trust chain).

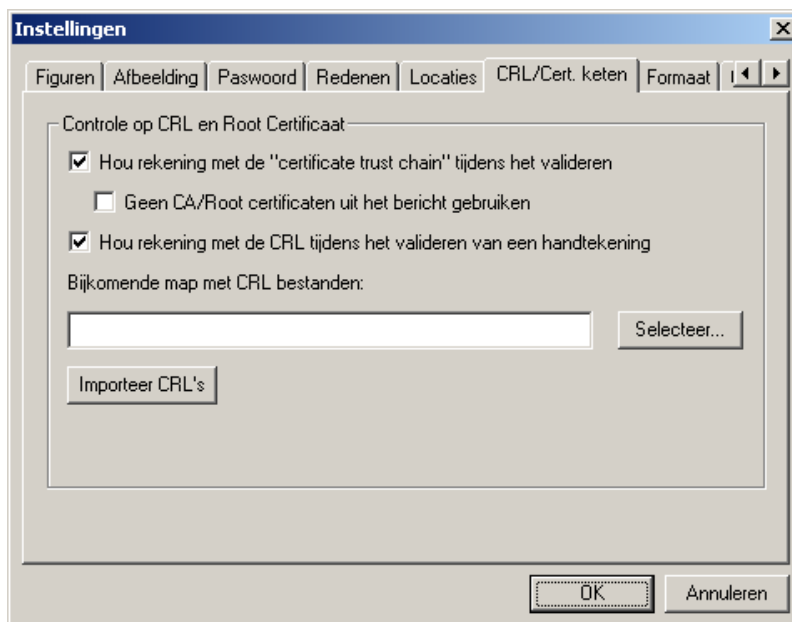
U kunt kiezen tussen:

- a. controle aan de hand van de CA/root certificaten die in het PDF document opgenomen zijn (2de checkbox niet aangeklikt)
of
 - b. controle aan de hand van de CA/root certificaten die bewaard zijn in de certificate store van Internet Explorer (2de checkbox wel aangeklikt)
- Controle op de eventuele revocatie van het certificaat van de ondertekenaar (CRL) en de uitgever(s) ervan.

Enkel de revocatie van certificaten met een CRL distributiepunt kan gecontroleerd worden. Indien u beschikt over een Internetaansluiting, wordt de CRL automatisch gedownload en op uw PC geïnstalleerd. Certificaten op de CRL zijn gerevoceerd en worden dan ook als ongeldig (vb. na verlies, diefstal, ...) aangeduid bij validatie.

Indien u niet beschikt over een Internetaansluiting, dan kunt u toch de revocatie van een certificaat als volgt testen:

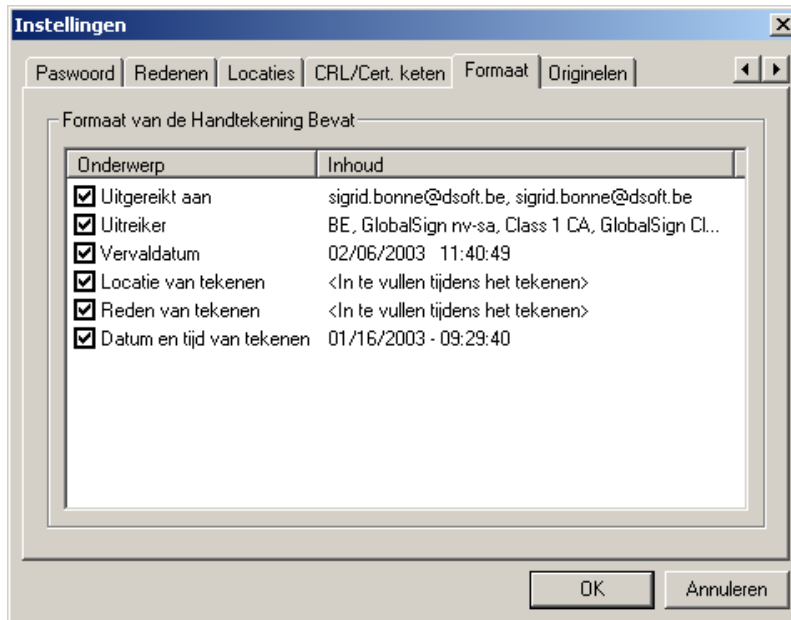
- Bijkomende CRL locatie:
Selecteer de locatie waar bijkomende geïmporteerde CRL's opgeslaan zijn en klik op 'Importeer CRL's' om deze te kunnen gebruiken.



3.8 Formaat

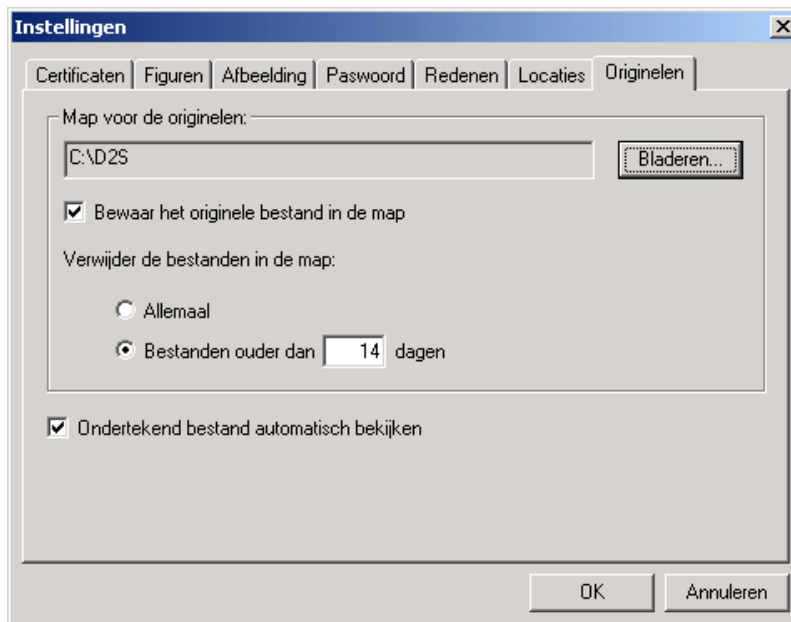
In dit venster kunt u specificeren welke tekst (volledige of verkorte vorm in 'Afbeelding'-tab, zie Afbeelding op pagina 11) de handtekening zal bevatten.

- In het 'Formaat van de Handtekening Bevat' veld kunt u de verschillende sleutels selecteren die u wil zien op het PDF document.



3.9 Originelen

In de 'Originelen' sectie kunt u een specifieke folder aanduiden waarin een kopie van het originele PDF document geplaatst wordt. Dit kan interessant zijn als u de originele versie van het PDF document wilt behouden of als u een back-up wilt hebben.




- Blader naar een folder om een kopie van het originele PDF document op te slaan.
- Selecteer 'Bewaar het originele bestand in de map' om een kopie van het originele document te bewaren.
- Kies voor 'Allemaal' als alle originele PDF files in deze map moeten verwijderd worden bij het opstarten van D2S Sign&Validate. De software verwijdert enkel PDF documenten in deze folder.
- Indien u 'Bestanden ouder dan ...' selecteert en het aantal dagen ingeeft, dan zal D2S Sign&Validate alle PDF documenten ouder dan het gedefinieerde aantal dagen uit deze folder verwijderen (na opstarten van de applicatie).
- Selecteer 'Ondertekend bestand automatisch bekijken' om na het ondertekenen, automatisch het PDF document te laten openen in Acrobat.

4 Handtekeningen

U kunt de eigenschappen van een handtekening bekijken in het 'D2S Sign&Validate' venster.


4.1 Valideren

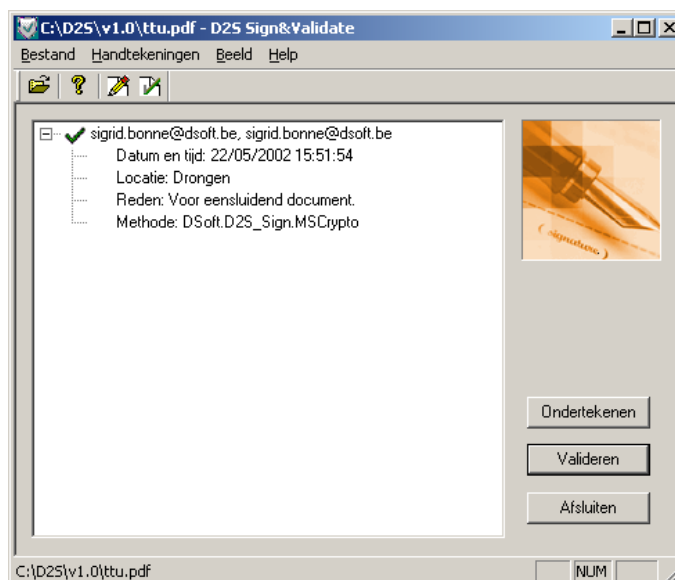
Een handtekening moet gevalideerd worden om te verifiëren dat het gesignde document niet is gewijzigd na ondertekening of om de identiteit van de ondertekenaar te bevestigen. Als u een handtekening toevoegt aan een document zal de informatie, die de ondertekenaar identificeert, toegevoegd worden. Als u een handtekening valideert zal deze informatie gecontroleerd worden.

- Kies 'Handtekeningen > Valideren' uit het menu of klik op de 'Valideren' knop naast het documentvenster, of klik op .

| Validiteitsstatus | Icoon in palet |
|--|---|
| Getekend, maar niet gevalideerd. |  |
| Geldig, maar de identiteit van de ondertekenaar kon niet gevalideerd worden. Controle op CRL en/of certificate chain is gevraagd maar niet mogelijk. |  |
| Geldig, en de identiteit van de ondertekenaar is ook gevalideerd. Controle op CRL en/of certificate chain is geslaagd indien gevraagd. |  |
| Ongeldig. Controle op CRL en/of certificate chain heeft gefaald indien gevraagd. |  |
| Document werd gewijzigd na ondertekenen. |  |

4.1.1 Nakijken van de eigenschappen van een handtekening

- Klik op  naast de handtekening om de details van de handtekening te bekijken. Deze eigenschappen verschijnen in het 'D2S Sign&Validate' venster.



- Naam:
naam van de certificaat houder
- 'Datum en tijd':
datum en uur wanneer de handtekening werd toegevoegd
- 'Locatie':
locatie van ondertekening (optioneel)
- 'Reden':
reden van ondertekening (optioneel)

4.1.2 Verifiëren van de volledige handtekeningdetails

- Selecteer en rechts-klik op een gevalideerde handtekening in het 'D2S Sign&Validate'-venster.
Het 'Eigenschappen van de Handtekening' venster verschijnt.



Geldigheid

- 'Handtekening geldig/niet geldig/onbekend': geeft aan of het bestand al dan niet reeds bewerkt werd.
- 'Controle op certificatie-ketting': geslaagd, niet mogelijk, niet gevraagd, gefaald
'Niet mogelijk' duidt aan dat de handtekening de CA en/of root certificaten niet bevat.
'Niet gevraagd' toont aan dat er geen controle is geweest. (zie CRL/Cert. Keten op pagina 15)
- 'Controle op CRL geldigheid': geslaagd, niet mogelijk, niet gevraagd, gefaald
'Niet mogelijk' duidt aan dat de CRL niet aanwezig is op het systeem. 'Niet gevraagd' toont aan dat er geen controle is geweest. (zie CRL/Cert. Keten op pagina 15)
- 'Controle op certificaat-revocatie': geslaagd, niet mogelijk, niet gevraagd, gefaald
'Niet mogelijk' duidt aan dat er geen enkele geldige CRL op het systeem werd gevonden.
'Niet gevraagd' toont aan dat er geen controle is geweest. (zie CRL/Cert. Keten op pagina 15) 'Geslaagd' betekent dat het certificaat op geen enkele geldige CRL verschijnt.
- 'Tijdstip van tekenen valt binnen geldigheid van het cert.': geslaagd of gefaald
Toont aan als de handtekening al dan niet werd gecreëerd binnen de geldigheidsperiode van het certificaat van de ondertekenaar.

Eigenschappen

- Ondertekend door:
naam van de ondertekenaar
- Datum:
datum en uur wanneer de handtekening werd geplaatst
- Reden:
reden van ondertekening
- Plaats:
plaats van ondertekening
- Details certificaat:
de instantie die de certificaten uitgeeft, vervalddag en dag van uitgave

4.2 Ondertekenen

- Kies 'Handtekeningen > Ondertekenen' uit het menu, klik op de 'Ondertekenen' knop naast het document-venster, of klik op .
- Het volgende venster verschijnt:



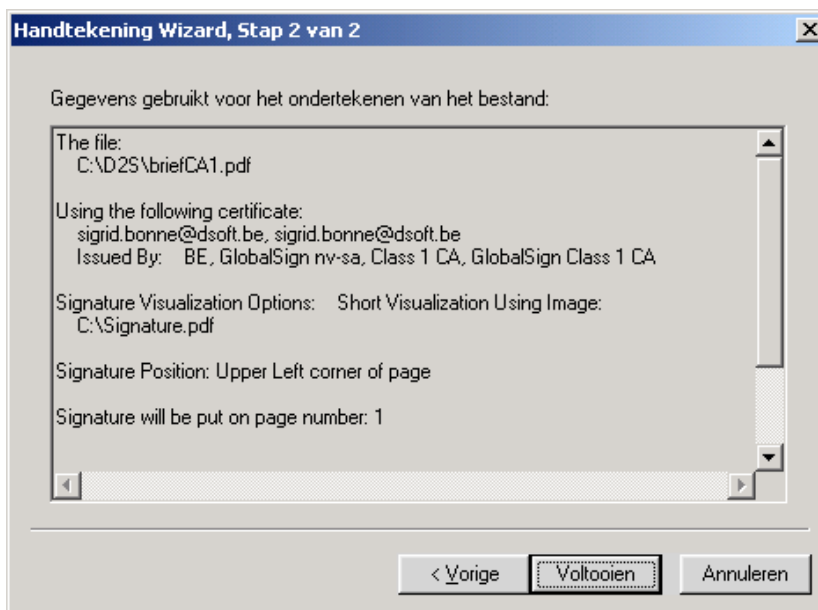
Certificaat gebruikt voor ondertekenen

- Klik op de 'Tonen...' knop om de eigenschappen van het gebruikte certificaat te bekijken.

Voorstelling

U kunt een afbeelding van de handtekening al dan niet laten verschijnen op het PDF document.

- Bij de volledige voorstelling verschijnt naast een afbeelding van de handtekening ook de datum en identiteit van het ondertekenen op het PDF document. Deze optie is enkel beschikbaar als een afbeelding van de handtekening geconfigureerd is. Standaard wordt de voorkeur instelling overgenomen (zie 3.3).
- Bij de verkorte voorstelling verschijnt enkel de datum en identiteit van het ondertekenen op het PDF document.
- Zonder voorstelling wordt het document wel ondertekend maar dit is enkel zichtbaar via 'Toon Handtekeningen' in Acrobat (niet in de Reader).

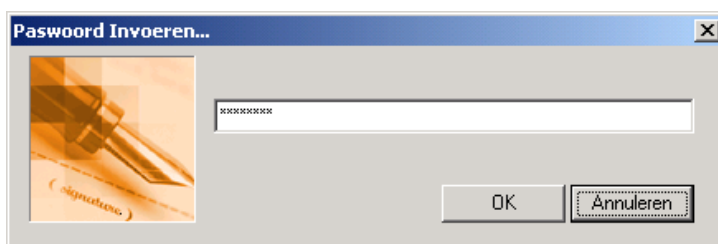


Bijkomende Informatie

- Kies de reden en locatie voor het ondertekenen indien gewenst. Deze lijsten kunnen gewijzigd worden in het 'Instellingen' venster (zie 3.5 en 3.6).
- Klik op 'Volgende' en stap 2 van de Handtekening Wizard verschijnt:

Een overzicht van de vooraf bepaalde instellingen verschijnt. Het PDF document zal ondertekend worden met deze parameters.

- Klik op 'Vorige' om eventueel een parameter te wijzigen.
- Klik op 'Voltoeien', het 'Opslaan Als' venster verschijnt om het document te ondertekenen. Het paswoordvenster verschijnt als dit vereist is volgens de instellingen (zie 3.4).



- Geef uw paswoord in en klik op 'OK'.
- Als dit de eerste handtekening is die aan een document wordt toegevoegd, dan zal het 'Opslaan Als' dialoogvenster verschijnen. Geef het document een naam en een plaats en klik op 'Opslaan'. De nieuwe handtekening verschijnt als laatste item in het documentvenster samen met het icoon dat aangeeft dat de handtekening geldig is. U kunt 'Opslaan Als' niet gebruiken op een ondertekend document.

5 Tips & Tricks

- Netscape gebruikers die D2S willen gebruiken moeten hun certificaat exporteren en dit importeren in de Windows CSP via 'Internet Explorer'.

Exporteer uw certificaat met Netscape:

- Open het 'Security Info' venster door op het 'Lock' icoon te klikken in de werkbalk. Selecteer 'Certificates' en 'Yours'.
- Selecteer het certificaat dat u wilt exporteren en klik op 'Export'.
- Een paswoord wordt gevraagd om de data te beschermen en een locatie wordt gevraagd om het geëxporteerde certificaat op te slaan.

Importeer uw certificaat met Internet Explorer:

- Selecteer 'Internet Options...' in het 'Tools' menu van Internet Explorer.
- Klik op 'Certificates...' in het 'Content' venster.
- Klik op 'Import...' en volg de richtlijnen op het scherm.
- Geef de locatie in van het bestand dat u in Netscape hebt gegenereerd.

Na het vervullen van deze verschillende stappen kan uw certificaat gebruikt worden met 'D2S Sign&Validate' (zie Instellingen op pagina 8).