globalcollect™

International Payment Services

User Guide - File Transfer
V1.4

Contents

1 GlobalCollect Contact Information

Contact us
GlobalCollect
P.O Box 2001
2130 GE Hoofddorp
The Netherlands
Telephone: +31 (0)23 567 1500
E-mail: info@globalcollect.com

Web site
Visit the GlobalCollect Web site www.globalcollect.com for information about the products and services of GlobalCollect including a demo.

2 Goal and Context

The User Guide File Transfer aims to give a full and good understanding of the File Transfer.

2.1 Overview of important documents

Administrative Guide
This Guide includes a description of the reconciliation model of GlobalCollect, explaining reporting periods, cut-off times, identifying references in online and offline interfaces and the relation between operational reports and financial reports.

Service Level Guide
This Guide contains an overview of the technical set-up, the service levels that GlobalCollect commits to, including the Maintenance Calendar.

Programmers Guide WebCollect
The technical guide for Merchant developers. This guide describes all interfaces and other technical aspects of our online platform.

Programmers Guide BatchCollect
The technical guide for Merchant developers. This guide describes all interfaces and other technical aspects of our off-line platform.

Programmers Guide Reporting
The technical guide for Merchant developers. This guide describes the reporting interface including sets of rejection, refusal and reversal codes.

User Guide File Transfer
The technical manual describing how to set up a Secure File Transfer account on the GlobalCollect SFT site. With this account Merchant are able to download the operational and financial report files of GlobalCollect.

User Guide Payment Console
The guide that describes the working of the online management tool for the Merchant without taking it to a technical level.

Network plus Network Glossary
An extensive sheet with all available payment combinations GlobalCollect can offer Merchant.

2.2 Version History

Version	Date Changed	Short Description
0.1	May 3rd, 2004	Draft version
1.0	May 7th, 2004	First version
1.2	Feb 4th, 2005	Changes in SSH
1.3	Feb 7th, 2006	Changes in signing up and contact

2.3 Disclaimer

GlobalCollect gives extensive attention to the content of this document but makes no warranties or representations about the accuracy or completeness of it. Neither GlobalCollect nor any of its affiliates shall be liable for any direct, incidental, consequential, indirect or punitive damages arising out of access to or use of any content of this document.

Because of the complexity of the process of direct debit and the right of banking institutions to alter conditions, this document can only serve as a description and is subject to modifications.

2.4 Suggestions

Suggestions regarding the content of this document are welcome and may be forwarded to GlobalCollect for the attention of the Development Team:

pdm@globalcollect.com

2.5 Questions

If you still have questions or problems please contact our customer service department.

CustomerServices@globalcollect.com

Introduction

The Secure File Transfer service (SFT) offers a secure way of exchanging file(s) over the Internet between GlobalCollect and its customers. It includes authentication (making sure that the other side is indeed who they say they are) and encryption (making sure that anything transmitted over the connection is unreadable for anyone that might intercept it).
You will be allocated your own input and output directories on our secure Internet server, where you can place your files and retrieve your reports from GlobalCollect. These directories will only be accessible for you and the GlobalCollect system. They are not accessible to anyone else.

Within the SFT service there are two flavours. You have to choose between ***Browser based secure file transfer*** and ***SCP based secure file transfer***.

- **Browser based secure file transfer**

This method of data transmission is based on the Secure Socket Layer (SSL3) protocol. It offers a user-friendly interface.
You can upload and download file(s), one by one, to and from your directories on our secure Internet server using an Internet browser (either Microsoft Internet Explorer 5.0 or higher, or Netscape Navigator 4.0 or higher). The only extra thing you need is a certificate (explained in more detail further on).
You will have to interact with your Internet browser to start uploads and downloads. There is no automatic way of doing this, either than using the other flavor of SFT, namely SCP.

- **SCP based secure file transfer**

SCP is part of the Secure Shell (SSH), probably the most used tool for remote management of UNIX servers. It uses public and private keys for authentication (no certificates needed), and sends or retrieves files encrypted over the Internet.
There are two ways to use SSH, either using a UNIX server (y*ou will need a UNIX expert to setup SCP on a UNIX server on your side*) or using SSH on a workstation (you probably will still need some UNIX knowledge to set it up).
Using scripts or by developing a simple UNIX daemon you can automate the use of SCP and thus automate file exchange between your system and the GlobalCollect SFT internet server. Global Collect supports version of SSH protocol v2.0 or higher.

3 Browser based secure file transfer

3.1 Overview

This chapter describes how you can obtain a client certificate at Verisign and authenticate yourself at the Global Collect SFT website. When you try to log on to the GC website, the website will ask for your certificate stored in your browser. This method is called “client authentication”, since your browser is used as a client to connect to the GC webserver. You don’t need to remember any username or password. Your certificate holds all the necessary information.

Another certificate at the website ensures that a secure link is set up between your browser and the GC webserver. All information sent between the GC website and your browser is encrypted. This means that your certificate information is not readable by third parties "listening" on the Internet. Also all data uploaded is secure.

3.2 What do you have to do?

Step A: Obtain a browser certificate
Such a certificate can be obtained from a so-called "Certification Authority", like for example Verisign or Thawte.

Step B: Send some specific user details from your certificate to Global Collect
GC stores these details in their website access database so the website knows you are authorized whenever you are trying to access the website. You will receive confirmation from GC when your user details are configured in the database.

Step C: Test your upload
You can test your upload by sending a few dummy files. GC will monitor your upload and present you with a report that you can download. If all is well, your account is activated and successfully tested.

Step D: Commence normal production
You can now upload your files and download your reports on a 7x24 basis.

3.3 How to obtain a client certificate for your browser?

3.3.1 Step 1: preparation

These steps assume you have a computer with Microsoft Internet Explorer version 4 or higher. If you do wish to use a Netscape browser, an information page is available at the end of this chapter.

Make sure you have a valid credit card ready. The costs of a client certificate are approx. $14.95 per year (price 2003). Please note that pricing may vary in different countries.

Make sure you have a valid Email address.

Make sure your browser has its security settings set to the default setting: "medium". You can check this by accessing in your browser tab the following sequence: tools => security => internet

Make sure you use the same browser for the entire process. Only the browser you use to obtain the certificate can be used to log into the Global Collect website. **Your browser needs to support SSL3 and support 128 bits encryption.** You will need to upgrade to higher version, If your browser does not support 128 bits cipher and/or SSL3.

3.3.2 Step 2: connect to the Internet

This can be done by using a dial-up connection or via your office network. If you do use the office network to obtain a certificate and you are using a proxy (which most corporate networks do) make sure the HTTPS protocol is enabled in the proxy. When in doubt contact your network administrator about this.

3.3.3 Step 3: go to Verisign

Type into your browser **www.verisign.com**

3.3.4 Step 4: select your digital ID

Click in the heading "Products & Services".
Select in the menu "Security Services" the field "Managed PKI Services".
Select in the menu "Product & Services" the field "PKI Applications" .
Select in the menu "Product & Services" the field "Digital ID's for Secure Email" .
Click on the Yellow button "Buy Now".

> The certificate you will generate is bound to your validated e-mail address and can be used to digitally sign your e-mail and receive encrypted e-mail. It can also be used by your Web browser as the equivalent of an electronic membership card or passport to identify you to participating Web sites that wish to restrict access, eliminating the need to remember usernames and passwords.

3.3.5 Step 5: Go to "Get your Verisign Digital ID now!"

Click again on the Yellow button "Buy now"
A new window will be opened.
Choose your browser.

3.3.6 Step 6: Fill in the open fields on this webform.

Please be careful when filling in the fields, all information will be stored onto your certificate. If you should enter wrong information on this form, you will have to apply for a new certificate.

Please note: Before you submit the form, it is a good idea to make a physical copy i.e. by printing the filled in webpage. This way you know the filled in fields for next year. It is vital that you use the same information each year, since Global Collect will have to reconfigure your account every time you use different information.

- Make sure you type a valid Email address.
  You might not want to use your personal Email address, but a generic one of the helpdesk of your organization. The reason for this is that when your certificate is about to expire, Verisign will send you an Email to tell you so. If you are no longer a member of this organization the organization will not be aware of this.

- Make sure you remember the password, which you type on the form.

- Please check the field "Choose Your Encryption Strength".
  It should state something like: "Microsoft base cryptographic provider". If this field is blanked out, the Verisign server is unable to detect your browser settings. The most common cause is that the proxyserver you use is disabling your browser type. Abort the process now and use a browser that has a direct connection between your computer and Verisign (for example through use of a modem).

- Also check the box to protect your private key.

When you press "accept" a small popup box will appear and mention that an RSA key has been generated. This is a warning generated by <u>your</u> browser. What happens is that the Verisign server has requested your browser to generate a public-private keypair. The private key is safely stored in your browser. The public key is send with the form to the Verisign website. With the information and the public key, Verisign can generate a personal certificate.

It is therefore important that you use the same browser when you apply for a certificate at Verisign. If you should apply for a certificate at Verisign at the office and then try to obtain the certificate via the browser at your home, the service will not work. Since your private key is on the office computer. In this particular case Verisign will generate an error if you try.

The private key together with the certificate enables you to send encrypted messages to other people and authenticate yourself at the GC website. Other people can verify your certificate at Verisign to see if it is a valid certificate. This way Verisign acts as a “trusted third party” between you and other people.

Press “OK” on the popup box.

3.3.7 Step 7: wait for an Email form Verisign to arrive in your Emailbox

Now wait for an Email from Verisign to arrive in your Emailbox
This should take a couple of minutes depending on how busy your corporate mailservers are. The Email will mention that you have a Digital ID PIN. Click on the URL in the Email wait for the webpage to load into your browser.

3.3.8 Step 8: Install the certificate

Click on “INSTALL”
The certificate will now load into your browser. This is an invisible process.
There have been cases that this step did not work. After clicking on “install” the browser generated a page: “URL not found” or “server is not responding”. Then press the “back” button of your browser and press try again.

Now you can use the certificate to authenticate yourself at the GC website. But first you need to check if the certificate is in place.

1. Go to the “tools” in your browser taskbar. Then select “internet options”. Then select the tab “content”.
2. Now click on the button “certificates”. A new menu should open.
3. As you can see a certificate with a name should be in your Certificate browser database.
4. Now double-click on the certificate. Another view with more detailed information on this certificate should open.
5. Click on the tab “Details”. Click once on “Subject”.
6. Here it is clear to see what information about you is present in the certificate. The capital letters all are part of the X500 international standard concerning personal identification.

E =	Email address
CN=	Common Name
OU=	Organizational Unit
O=	Organisation

Sometimes there is a capital C for Country too.

It is this information that the Global Collect site will need to know in order to authenticate you. For Global Collect to receive this information, you will need to send the information to them via Email. You can do this in the following manner. Now move your mouse to the E= and move your mouse over the entire text while holding the left mouse button.

Please note: make sure that all the information is included.

Now release the mouse button and press the ctrl (control) key and hold it. Now press the key c. The text is now copied into the Windows text buffer.

Now continue with the next chapter “Send your certificate information to GlobalCollect”.

3.4 Send your certificate information to GlobalCollect

Now open your Email client (for example Outlook) and send a mail to sft-info@globalcollect.com.

Make sure the subject mentions “new SFT account”. Then in the body of the mail press ctrl and the key v. The information which was stored in your Windows text buffer is now pasted into your Email.

You will also have to provide a contact person with a telephone number.

Now send the Email. Within a few days you should receive an Email from GlobalCollect with further instructions.

How to use the browser based secure file transfer

3.4.1 Adviced security settings for your browser

You are free to set your browser settings as you wish. However, you will have to enable Java. We advice you to contact your own system administrator for the security settings.)

3.4.2 Connecting to the GlobalCollect secure web server

Go to the web address **https://sft.globalcollect.com** ***Notice the 's' in 'https'.***

Depending on your browser settings, you will get a message saying you are about to view pages over a secure connection.

Next you will get a window where you can select the cetificate you want to use to connect to the GlobalCollect secure web server. You will have to choose the certificate, which information you provided to GlobalCollect. If you only have 1 certificate ……..
Click OK and you will get a window saying 'data is being signed with your private key'. This means that data on this connection is now being encrypted before it is sent.

Click OK en you see the SFT download page in your browser.

Notice the 'lock' at the right bottom of your browser window. The lock indicates that you have a secure connection. When you double click on the 'lock' you will get the certificate information of the server with which you have this connection.

3.4.3 Downloading files

Click on 'Download', at the left of the window. You will see a list of files on the SFT download page. These are the files you can download and/or delete.
You can also display the download log. This log display your last 100 downloads. Click 'View Log' to display the log.

Start of a download will be logged as DOWNLOAD.
A failure during a download will be logged as CANCEL.
A delete of a file will be logged as DELETE.
Click on 'back' to go back to the SFT download page.

Note: If log is empty, press Refresh button in browser. (Workaround for bug when sometimes log is not shown).

To download a file, select it and click download.
Select 'Save this file to disk' and click OK.
Now select the directory where you want the file to be placed and click 'Save'. A status window will appear.

Depending on your browser settings the status window will stay on the screen after completion of the download. You have to click 'Close' to proceed. Then you will be returned to the SFT download page.

Deleting files on the GlobalCollect secure web server works in a similar way. Select the file and click 'Delete File'. The SFT download page will then be shown again, and the deleted file will have been removed from the file list.

Notice: All files older then 1 month will be deleted by the server automatically.

3.4.4 Uploading files

To upload files click on ‘UPLOAD’ at the right on the page. You will see a window, depending on your browser settings, with a securior warning.

This window warns you about the fact that the GlobalCollect secure web server want to install and run a Java applet on your machine. Click ‘Yes’ to proceed and the SFT upload page will appear.

To upload files you will first have to add files to the file list. Click on ‘Add to list’ to add a file to the file list.

Go to the directory where the file you want to upload is located and select the file. Than click on ‘Open’. You will be returned to the SFT upload page, and the file will have been added to the file list.
Repeat this for all the files you wish to upload.

If there should be a file in the list you do NOT want to upload, you can remove it from the list by selecting the specific file and clicking on ‘Remove from list’.
To start the upload of the files in the file list, just click ‘Start Upload’. A status message will appear (and change when the upload process status changes.

Once the upload process is completed the status message will display the ‘Finished Upload’ message.

Note: If log is empty, press Refresh button in browser. (Workaround for bug when sometimes log is not shown).

Click ‘Continue’ to return to the SFT upload page.

You can also display the upload log. This log display your last 100 uploads. Click ‘View Log’ to display the log.

Note: Whenever an upload failed or was canceled, the upload will not be logged. Only succesfull uploads are logged.
Click on ‘Back’ to return to the SFT upload page.
Note: if the log is empty, press or click <REFRESH> in your browser (this is a work-around for a bug that sometimes the log is not shown)

3.4.5 Disconnecting from the GlobalCollect secure web server

To disconnect from the GlobalCollect secure web server you can either close/exit the browser or connect to another web server/site (for example clicking on the ‘Home’ button).
Depending on your browser setting you will get a window which indicates that you are leaving a secured Internet Connection.
Click ‘Yes’ to proceed.

3.5 Netscape issues

If you wish to use Netscape as a browser the process is almost identical to the use of a Microsoft browser. However, there are a few differences….

- Make sure you use a Netscape browser version 4.x or higher
- When you generate a private / personal key in your Netscape browser, Netscape wants you to create a personal certificate database in your browser. This database is protected by a personal password.
- Every time you access Global Collect and the website requests your personal certificate, Netscape will ask you for your database password.

The reason for this is that when your computer is stolen, the thief cannot automatically use your personal certificate. The database is protected by 3DES encryption and it will take a millennium to crack it with a brute force attack.

From a security perspective the request for a personal password is valid, since without passwords you are authenticating a computer not a person.

- You can access your certificate via the “security” button on the top of your browser. It is the button with the picture of the lock on it.
- You should then click on “yours”, a view with a list of all certificates will be displayed. Click on your certificate once and press the button view.

Now a new popup is opened. On the right side of the popup information about the signing organization will be displayed. Very likely this will be information about Verisign.

On the left side of the popup personal information about you is displayed. It is this information that Global Collect needs to activate your account on the Global Collect website. Please cut and paste this information into an Email. Send the information to sft-info@Emailglobalcollect.com

Global Collect will get in touch with you with further instructions.

4 Frequently Asked Questions (FAQ) Browser based SFT

As the SFT service is still very new there are not much frequently asked question yet. This chapter will be filled as more questions arrive.

4.1 Connecting with a Nescape browser via a proxy server

Description

The uploading of files via a proxyserver will not work with Netscape browsers.

Cause

This has to do with the Netscape browser not being able to pick up environment variables like the proxy settings and always try to set up a direct connection with the Global Collect website.

Resolution/workaround

There is a very simple work around.

1) Open your Hosts file which can be found in c:/windows when using Windows 9x or c:/winnt/system32/drivers/etc on a Windows NT machine.

The host file will look like:

```
# Copyright (c) 1998 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP stack for Windows98
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
127.0.0.1       localhost
```

2) Now enter the following line at the end of this file.

```
    1.2.3.4           sft.globalcollect.com
```

What will happen is that the Netscape browser will try to connect directly to the Global Collect website. It will look into the host file, find a referencing IP address, and forget all about the number 1.2.3.4. And try to connect via the proxyserver in a normal way. This is a fairly crude solution, but it works.

4.2 File extension problem when downloading

Description

In some circumstances (using Internet Explorer), when downloading a file, the extension of the downloaded file may get corrupted. When you download (for example) a file with the extension "**.EC1**", the file is saved with the extension "**.EC1..EC1**".

Cause

Unkown. This might be a bug in Internet Explorer, but it might also be a problem within the java applet.

Resolution/workaround

By adding the file extension type to the known file extensions on your windows installation, you have a workaround for this problem. The following example shows how to do this for the file extension "**EC1**".

1. Start the windows explorer and choose "View" and then "Options":
2. Choose "File Types":
3. Choose "New Type":
4. Fill in the window as follows:
   - Description of type: GC Repoprt
   - Associated extension: ec1
   - Content type: text/plain
   - Default extension: txt
5. Click "OK". You will now see the file in the list.
6. Click "OK". The problem will not occur anymore for this file extension type.

4.3 Browser states 40 bit encryption

Description

My browser states that the https://sft.globalcollect.com uses a 40bit encryption. At this moment 128bit encryption is freely available. Why are you not using 128bit encryption?

Cause

We do use the 128bit encryption. Probably your browser does not have the 128 bit encryption installed. To see what encryption your browser uses, move your mouse over the lock at the bottom of the window. A tooltip should appear (in yellow) that states the currently used encryption.

Resolution/workaround

Upgrade your browser to use 128 bit encryption. To do that click 'help' in your browser and then select 'info'.

If 'cipher Strength' states something else than 128 bit, then follow the 'update information' link and follow the instructions to upgrade your browser.

4.4 The uploading of a file takes a long time

Description

The uploading of a file takes a long time. When I press the “Start Upload” button a new window pops up and states that it is uploading but nothing seems to happening. Why is this?

Cause

The time your computer needs to upload the file depends on
1) the processing power of your computer,
2) how large the file is you want to upload,
3) how much bandwidth is available to you.

In general the bandwidth will not be a bottleneck. For reference purposes we have included a timetable.

File size (kilo bytes)	Download time with Pentium III
50kb	6 - 10 seconds
100kb	7 - 15 seconds
200kb	20 - 40 seconds
500kb	30 - 45 seconds
1000kb (= 1Mb)	40 - 50 seconds

Resolution/workaround

Use a newer PC with more processing power.

4.5 Netscape does not recognize the certificate authority

Description

I connect to https://sft.globalcollect.com and my browser states that the website uses a New Site Certificate and Netscape does not recognize the authority who signed the certificate. What is this?

Cause

This happens when the Certificate Authority is unknown to your browser. Global Collect uses a Dutch Certificate Authority.

Resolution/workaround

To prevent the warning from coming up every time you connect to the website do the following:

- Click on “next” twice when the warning appears
- When it says “Are you willing to accept this certificate for the purposes of receiving encrypted information from this web site?” Select the radiobutton: “accept this certificate forever”.

You will now not longer receive the warning

4.6 Using your certificate on an other PC

Description

My PC is being replaced. How do I make sure I can use SFT on the new PC.

Resolution

You will have to export your certificate from the old PC and import it on the new one. **Make sure you remove your certificate from the old PC.**

Export digital certificate with Internet Explorer

- In Internet Explorer, select Internet Option... under the Tools menu
- Select the Content tab and click the Certificates... button
- Select the certificate that you want to export
- Click the Export... button
- Follow the Certificate Manager Import Wizard and enter the password to encrypt the private key when prompted
- Enter the file name you want to export

Import digital certificate with Internet Explorer

- In Internet Explorer, select Internet Option... under the Tools menu
- Select the Content tab and click the Certificates... button
- Click the Import... button
- Follow the Certificate Manager Import Wizard and enter the password to access the file when prompted

Remove digital certificate with Internet Explorer

- In Internet Explorer, select Internet Option... under the Tools menu
- Select the Content tab and click the Certificates... button
- Select the certificate that you want to remove
- Click the Remove button

4.7 Windows XP

Windows XP does not support Java. You have to down-load Java tools from the site of Microsoft.

4.8 Other questions or remarks

If you still have questions or problems please contact our customer service department.

CustomerServices@globalcollect.com

5 Secure Copy Protocol (SCP) based secure file transfer

5.1 Overview

To send data to Global Collect via the Internet, you can use Secure Copy Protocol (SCP). SCP is part of the Secure Shell (SSH), probably the most used tool for remote management of UNIX servers. Global Collect supports version of SSHv2.0 or higher (e.g. OpenSSH3.9p1). SSH ensures that a secure session between your server and the server from Global Collect is established on Port 22. When the session is in place, SCP can be used to “tunnel” data through this session. Furthermore this chapter does assume that you have a basic knowledge of UNIX. The examples use the generation of RSA keypairs but also DSA keypairs are supported.

5.1.1 What do you have to do?

Step A: Sign up for the SFT SCP service
Contact Implementation department at Email sft-info@globalcollect.com to sign up for the SFT service.

Ask Global Collect to setup your directories and to give you a userid and password, and setup directories for you on the GlobalCollect secure Internet server. You also will have to provide a contact person with a telephone number.

Step B: Install SSH (including SCP) on your System
This step includes getting a SSH package from the internet www.openssh.org (or otherwise) and installing it on your system.

Step C: Test your SCP connection
This step includes setting up a SCP connection and sending a test file to the GlobalCollect secure Internet server.

Step D: Automate the file exchange (optional)
This step includes exchanging public key between your server and the GlobalCollect secure Internet server, and testing if you can send and receive files without having to provide a password. Subsequently you can automate the process using scripts (or writing an application) to execute the SCP commands.

Step E: Commence normal production
You can now upload your files and download your reports on a 7x24 basis.

5.1.2 What do you need?

SSH v2 or higher
Possible free solutions are openssh for UNIX, which can be found at: http://www.openssh.org and putty for Windows, which can be found at:
http://www.chiark.greenend.org.uk/~sgtatham/putty/.

We recommend that you use SSHv2 or higher, for security reasons. For workstations we recommend the ‘SSH Tectia’ from ‘SSH Communications Security’ (www.ssh.com).

5.2 SCP using a (windows) workstation

5.2.1 Step A - Sign up for the SCP based SFT service

Contact Implementation department at Email sft-info@globalcollect.com to sign up for the SFT service.

Ask Global Collect to setup your directories and to give you a userid and password, and setup directories for you on the GlobalCollect secure Internet server. You also will have to provide a contact person with a telephone number.

5.2.2 Step B - Install SSH (including SCP) on your system

Just follow the installation instruction of the 'SSH Tectia' software package.

5.2.3 Step C - Test your connection

After downloading and installing the client for Windows, you should have 2 icons on your desktop: "SSH Secure Shell Client" and "SSH Secure File Transfer". To test the connection with GlobalCollect double-click "SSH Secure Shell Client".

Select from the File menu the option Connect.

In the following popup make sure the following are correctly filled in:
"Host Name" should be the sft.globalcollect.com or if you do not have a DNS the ip-address 147.29.80.58 "User Name" should contain the username assigned to you by GlobalCollect. "Port Number" is 22 and "Authentication Method" is Password.

After pressing the "Connect" button the connection with the GlobalCollect-server will be established.
If this is your first connection to our server you probably will be confronted with a question about Host Identification.

After supplying your assigned password, you will be logged in to our server. You will see the following screen:

The text in this screen will no longer be greyed out, and the status bar (underside of the screen) will say "Connected to sft.globalcollect.com".
You now have a working connection to our server. To start transferring files choose "New File Transfer" in the Window menu:

From here you can transfer files by dragging them in or out of this window, just like in the explorer.

5.2.4 Step D - Automate the file exchange on a workstation

5.2.4.1 Step 1 - Automate the authentication on a workstation

If you would rather not type the password every time you log in to our server, you can use the public key method. This means you generate a keypair, and one part (the public key) will be transferred to our server. From that moment on, you can log on without supplying the password.

Is this secure? Yes. Even more than the password method. Using a keypair, everything our server sends back will be encrypted with the public key. This can only be decrypted with your private key, which is only on your system.

To generate a keypair, start the Secure Shell Client and make a connection as previously explained.
Now select under the menu Edit the option Settings:

Select (on the left side) of the following window the option “User Keys”. Press the button “Generate New Keypair”. After pressing “Next” on the next screen, the computer will ask you for the key properties:

Make sure the “Key Type” is RSA, the “Key Length” is 1024 and protocol is SSHv2 and press “Next”. The computer will now calculate your key. After the process has finished press “Next” again. You will be prompted for some values.

In the field “File Name” fill a filename to your choice in. In the field “Comment” fill the comment in you would like. Make sure both fields “Passphrase” are empty.
Press “Next”.

You will be prompted whether you are sure about the empty passphrase. Press “Yes”.

The key generation is finished, now upload it to the GlobalCollect server by pressing “Upload Public key”. You will be asked some questions. Set the field “Public Key file” to rsa_key.
Set the field “Destination folder” to .ssh (it will contain the value .ssh2 by default).

Then press “Upload”. The public key will be put on the GlobalCollect server. Before you can login with your private key you will have to convert the public key. Go back to the SSH screen and type the following commands:

```
cd
cd .ssh
ssh-keygen -i > authorized_keys2
```

On the question “Enter file in which the key is” type rsa_key.pub and press enter. Note that if you make a typing error you will have to use the Delete key instead of Backspace to correct the error. The screen displays the conversion of the key:

Now everything is ready for public key authorization. Disconnect from the GlobalCollect server (type exit + ENTER), and try to connect again. This time when you are confronted with the screen “Connect to remote host” fill in the following:

For “Host Name” fill in sft.globalcollect.com or 147.29.80.58
For “User Name” fill in your assigned user name.
“Port Number” should be 22.
“Authentication Method” has to be “Public Key”.

The connection should proceed without prompting you for a password.

5.2.4.2 Step 2 - Automate the upload and download on a Workstation

Under Windows you can write a batch file to do your file transfers. For this to work you must have generated a keypair according to the explanation in the previous chapter. The following commands must be executed from a DOS window.

You will find a program called scp2.exe in the directory where you have installed SSH; default "C:\Program Files\SSH Communications Security\SSH Secure Shell".
You can execute this in the following way:

```
SCP2 /PATH/TO/LOCAL/FILE USERNAME@SFT.GLOBALCOLLECT.COM:IN/FILE
```

IN THIS COMMAND SUBSTITUTE "/PATH/TO/LOCAL/FILE" WITH THE FILE(S) TO TRANSFER, SUBSTITUTE USERNAME WITH YOUR ASSIGNED USERNAME AND SUBSTITUTE "REMOTE/PATH/TO/FILE" WITH THE LOCATION ON OUR SERVER. IF YOU ARE UPLOADING THIS SHOULD BE "IN/". IF YOU HAVE CREATED THE KEYPAIR, THE FILE WILL BE UPLOADED WITHOUT PROMPTING FOR A PASSWORD.

To download something, try:

```
SCP2 USERNAME@SFT.GLOBALCOLLECT.COM:OUT/FILE /LOCAL/PATH/TO/FILE
```

Here also substitute username with your assigned username, "remote/path/to/file" with the file to download and "/local/path/to/file" with the local path.
For downloading this should be: `scp2 username@sftglobalcollect.nl:out/* .` to retrieve all files ready in your directory to the local directory.

5.3 SCP using a UNIX server

5.3.1 Step A - Sign up for the SCP based SFT service

Contact Implementation department at Email sft-info@globalcollect.com to sign up for the SCP based SFT service.

Ask Global Collect to setup your directories and to give you a userid and password, and setup directories for you on the GlobalCollect secure Internet server. You also will have to provide a contact person with a telephone number.

5.3.2 Step B - How do I install SSH on a UNIX system?

From one of the above mentioned websites you can download the SSH binary. If you downloaded the source, you will need to compile the binary yourself. For compiling you might use GCC (GNU C Compiler). Help with compiling the binary is available on: http://www.ncsa.uiuc.edu/General/CC/ssh. There also is platform specific help available.

Other resources on SSH are:

- SSH FAQ on: http://wwwfg.rz.uni-karlsruhe.de/~ig25/ssh-faq
- Archive support for SSH: www.deja.com. Look for the newsgroup: comp.security.ssh
- More help on SSH is on http://www.openssh.com

Pre-compiled binaries are available on various websites. Via a search on the internet you can find the version for your platform. A word of warning is however appropriate. Some pre-compiled versions are put there by hackers and contain a so-called “backdoor”. Through use of this backdoor it is possible to gain root access to your system. We strongly recommend you to download and compile SSH yourself.

The sft.globalcollect.com server runs OpenSSH. We recommend that you also use OpenSSH as a client. Commercial clients will also work but there are some differences in the configuration of automatic upload. The examples in this chapter are created with OpenSSH client 3.1p1 on a HP UNIX system.

5.3.3 Step C - Connecting from your Unix server

Before you try to connect to the sft server you should create a ssh config file. This file contains some default values that make the use of SSH a little easier. In your home directory create a directory .ssh and set the permissions to rwx------:

```
cd
mkdir .ssh
chmod 700 .ssh
```

In the directory you just created create a file named config with the following lines:

```
Protocol 2
IdentityFile ~/.ssh/id_rsa
```

If you intend to generate a DSA keypair use id_dsa instead. Make sure you are hooked up to the Internet. Test the connection to the Global Collect server by trying to SSH the Global Collect server. SSH uses TCP port 22. This port must be open from your server to the Global Collect server. The command for invoking SSH is:

```
ssh –l <youraccountname> sft.globalcollect.com
```

or, if you do not have a DNS configured:

```
ssh –l <youraccountname> 147.29.80.58
```

The command for uploading a file has the following format

```
scp localdir/to/filename user@host:out/filename
```

The destination filename is optional but the colon after the hostname is required!

Example

```
ssh -l merchant sft.globalcollect.com
```

You will get the following response:

```
The authenticity of host 'sft.globalcollect.com (147.29.80.58)' can't be established.
RSA key fingerprint is 44:bb:14:67:51:22:5c:1e:a0:eb:54:07:b9:64:cc:8e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'sft.globalcollect.com,147.29.80.58' (RSA) to the list of known hosts.
merchant@sft.globalcollect.com's password: <password>
Last login: Fri Jun  7 11:18:14 2002 from 20.60.98.85
Sun Microsystems Inc.   SunOS 5.8       Generic February 2000
Sun Microsystems Inc.   SunOS 5.8       Generic February 2000
$
```

The first time you connect to the sft server you will be asked if you want to add the RSA fingerprint to the list of known hosts. Verify that the fingerprint is the same as in the example and answer yes. If you use SSH protocol 2 the fingerprint has to be (after 28-2-2005): 44:bb:14:67:51:22:5c:1e:a0:eb:54:07:b9:64:cc:8e. Before 28-02-2005 the fingerprint will be 4b:8a:b5:7d:26:f4:5e:9b:53:4d:7e:59:6e:3a:09:f3. If the fingerprint is not the same as above please contact Global Collect.

After this you are logged in to the sft.globalcollect.com server. Type exit to logout. For troubleshooting purposes you can use the flag -v (verbose):

```
ssh -l merchant sft.globalcollect.com
```

SSH will generate a lot of output that may give you a hint on what is happening. Make sure you have the output of SSH with the –v option available before you contact the Global Collect helpdesk.

Example

```
scp test.txt merchant@sft.globalcollect.com:in/test2.txt
```

You then receive feedback what SCP is doing. An example of the output is the following:

```
merchant@sft.globalcollect.com's password: <password>
test.txt             100%
|***************************************************************************|    16
00:00
```

If you are able to upload a file into in, congratulations. Unfortunately you have to sit behind your keyboard to enter a password every time you make a connection. Naturally you would like to automate this.

5.3.4 Step D - Automate the file exchange on UNIX

The above mentioned example is not suitable for uploading automatically. SCP will continue to ask for a password. A word of warning:

```
scp –v file merchant@sft.globalcollect.com:in < yourpassword
```

Will NOT work!

The example below describes a case of two servers (server sft.globalcollect.com and server Yourserver). Server Yourserver would like to upload files to server sft.globalcollect.com. The example describes the setup for OpenSSH. The setup for commercial SSH versions requires a conversion of the public key, please refer to chapter ????? for instructions on this.

5.3.4.1 Step 0: preperation

Please read all the steps before you start configuring. As you then know what you are doing.

5.3.4.2 Step 1: generate an RSA keypair on the Yourserver

Login onto Yourserver as a user. Make sure this user has a home directory. Don't *su* to become superuser. We advise you not to generate keys with root, this regarding to the safety of your system. In these steps you change "gcuser" in your provided user-id.

For OpenSSH Protocol version 2 the procedure is:

1. Execute the following command:
   ```
   ssh-keygen -t rsa
   ```
   In order to generate a dsa keypair change rsa into dsa.
2. At the question in which file to save the key, just press enter. You will be asked for a passphrase, press enter (do not type anything). Press enter again when asked for confirmation of the passphrase.
3. Copy the public key to sft.globalcollect.com, from your home-directory execute:
   ```
   scp .ssh/id_rsa.pub merchant@sft.globalcollect.com:
   ```
   Replace merchant with the user-id that was given to you by GlobalCollect. Don't forget the colon at the end or nothing will be copied and no error message will appear on the screen!
4. After providing your password, your public key will be copied to the globalcollect server.

5.3.4.3 Step 2: SSH from Yourserver to the sft.globalcollect.com server

1. Connect to the sft.globalcollect.com server:
   ```
   ssh -l gcuser sft.globalcollect.com
   ```
2. You are now in your home-directory on the globalcollect server. It will be something like /export/content/sglobal/klanten/12345678. Your directory should have the following structure:

/in	in this directory you can upload your files
/out	in this directory you can download your report files
3. Now install your public key. First create a directory .ssh if it doesn't already exist and set the permissions to rwx------:
   ```
   mkdir .ssh
   chmod 700 .ssh
   ```
   Make sure that your home directory (that is the directory that contains the .ssh subdirectory) is not writable for anyone but you. Execute the following command to set the permissions on your home directory:
   ```
   cd
   chmod 750 .
   ```
   (don't forget the dot in the last command)
   Move the key to the .ssh directory, from your home directory execute the command:
   ```
   mv id_rsa.pub .ssh/authorized_keys2
   chmod 644 .ssh/authorized_keys2
   ```
4. Type `exit` to log out.

5.3.4.4 Step 3: Test if you can SSH from Yourserver to sft.globalcollect.com in an automated way

Use the following command to login:

```
        ssh -l merchant sft.globalcollect.com
```

You should see something like:

```
Last login: Fri Jun  7 14:22:48 2002 from 20.60.98.85
Sun Microsystems Inc.   SunOS 5.8       Generic February 2000
Sun Microsystems Inc.   SunOS 5.8       Generic February 2000
$
```

You are now logged in from Yourserver to sft.globalcollect.com without using passwords. If you can't login without a password you can try to use the –v option with ssh. This will generate a lot of output that may give you a hint on what is going wrong.

5.3.4.5 Step 4: SCP from Yourserver to sft.globalcollect.com in an automated way

If you can login autimatically you can set up automatic file transfer to and from the sft server. For example if you want to transfer a file test.txt to the in directory on the sftserver execute the following command:

```
        scp test.txt merchant@sft.globalcollect.com:in
```

The response will be something like:

```
test.txt             100% |********************|    16       00:00
```

The file test.txt has successfully been transferred from Yourserver to sft.globalcollect.com.

5.3.4.6 Step 5 - Downloading in an automated way

This works exactly the same way as uploading. Here is the format:

```
        scp yourname@sft.globalcollect.com:in/remotefilename filenameonyourcomputer
```

Example:

```
        scp merchant@sft.globalcollect.com:in/test.txt test.txt
test.txt             100% |********************|    16       00:00
```

Please note:

```
        scp -v test.tar.gz merchant@sft.globalcollect.com:out
```

Don't forget to mention your destination directory (out in this example) where you have write permissions with user merchant. If you forget to mention the destination directory, the following will happen:

```
bash-2.02$ scp -v test.tar.gz merchant@sft.globalcollect.com
Executing: exec cp test.tar.gz merchant@sft.globalcollect.com
```

Something appears to be happening, but in actual fact, nothing is happening, Yourserver is unable to write into the proper directory on sft.globalcollect.com.

5.3.5 Additional information

5.3.5.1 What does /etc/ssh_config look like on Yourserver?

SSH has a system wide configuration file that is located in /opt/openssh2/etc/ssh_config (the location may differ with your installation). The settings in this configuration file can be overriden by the configuration file in .ssh/config in your home directory (see ???). Below is a sample configuration file for OpenSSH 2.

```
#       $OpenBSD: ssh_config,v 1.8 2001/02/02 12:57:51 deraadt Exp $

# This is ssh client systemwide configuration file.  See ssh(1) for more
# information.  This file provides defaults for users, and the values can
# be changed in per-user configuration files or on the command line.

# Configuration data is parsed as follows:
#  1. command line options
#  2. user-specific file
#  3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

# Site-wide defaults for various options

# Host *
#   ForwardAgent no
ForwardX11 yes
#   RhostsAuthentication no
#   RhostsRSAAuthentication yes
#   RSAAuthentication yes
#   PasswordAuthentication yes
#   FallBackToRsh no
#   UseRsh no
#   BatchMode no
#   CheckHostIP yes
#   StrictHostKeyChecking yes
#   IdentityFile ~/.ssh/identity
#   IdentityFile ~/.ssh/id_dsa
#   IdentityFile ~/.ssh/id_rsa1
#   IdentityFile ~/.ssh/id_rsa2
#   Port 22
#   Protocol 2,1
#   Cipher blowfish
#   EscapeChar ~
```

5.3.5.2 Logging in without passwords is that safe?

Well, if someone were to hack Yourserver and gain access to user merchant, the hacker would be able to access sft.globalcollect.com via your account. This is your responsibility.

To make it even secure, you could use ssh-agent. Read www.openssh.com for more information on this subject.

5.3.5.3 Going from SSH 1 to SSH 2 on Unix

If you upgrade your version of SSH (or OpenSSH) from version 1 to version 2, you will have to generate new keys. This can be done by following the procedure outlined under the paragraph "Automate the file exchange under Unix". There is no need to remove the previous keys, but you may do it, so logging in with the old keys is not allowed any more.