Consiglio Nazionale delle Ricerche

*T*he Security Procedure for Information Management on INDUCE Web-Server

Daniele Azzarelli, Massimo Martinelli, Ovidio Salvetti

B4-13

lug-2000

Project N° BE 97 - 4057
Contract N° BRPR - CT98 - 805

Date: 15.06.2000	Reference N°:	TR-2140-IEI-02	Revision:	1	Pages:	1/12
					Annexes:	-

The Security Procedure for Information Management on INDUCE Web-Server

Daniele Azzarelli, Massimo Martinelli, Ovidio Salvetti

IEI-CNR
Pisa Research Area, S. Cataldo
Via Alfieri 1, 56010 Ghezzano SGT (Pisa)

Summary

Project N° BE 97 - 4057
Contract N° BRPR - CT98 - 805

Date: 15.06.2000	Reference N°:	TR-2140-IEI-02	Revision:	1	Pages:	3/12
					Annexes:	-

Aim of this document

The aim of this document is to present the procedure that the INDUCE Partners can follow to read and write information from/into the Web-Server in a secure way.

Scheme of the PROCEDURE

The procedure for activating the *secure communication protocol* is shown in the Figure 1. In the scheme, the different operations and their relationships are evidenced.
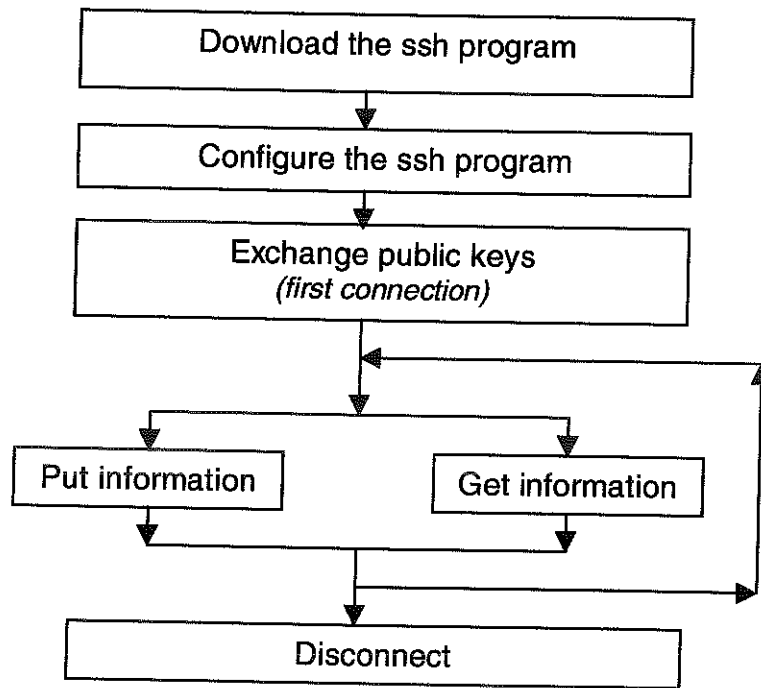
```
┌─────────────────────────────────┐
│   Download the ssh program      │
└─────────────────────────────────┘
               │
               ▼
┌─────────────────────────────────┐
│   Configure the ssh program     │
└─────────────────────────────────┘
               │
               ▼
┌─────────────────────────────────┐
│      Exchange public keys       │
│       (first connection)        │
└─────────────────────────────────┘
               │
               ▼
   ┌──────────────────┐        ┌──────────────────┐
   │  Put information  │        │  Get information  │
   └──────────────────┘        └──────────────────┘
               │                        │
               ▼                        ▼
        ┌─────────────────────────────────┐
        │          Disconnect             │
        └─────────────────────────────────┘
```

Figure 1 – Overall scheme of the security procedure.

Date: 15.06.2000	Reference N°:	TR-2140-IEI-02	Revision:	1	Pages:	4/12
					Annexes:	-

Basic Resources

Reading information from the site does not require any special software.

On the contrary, writing information into the site (i.e, storing documents in the *private environment*) requires *ad hoc* instruments; among the different possibilities, we suggest to use a third-part product called ssh.

In the following, the procedure to get the program is detailed.

Firstly, you need to download the ssh program by connecting to the site

http://commerce.ssh.com

taking care to select the *Non-Commercial SSH Secure Shell for Workstations*.
During this operation some information are requested before starting the download.

System Configuration

After the program has been downloaded and installed on your computer, run it and then select the "Setting" choice from the Edit menu. Then select "User Keys".
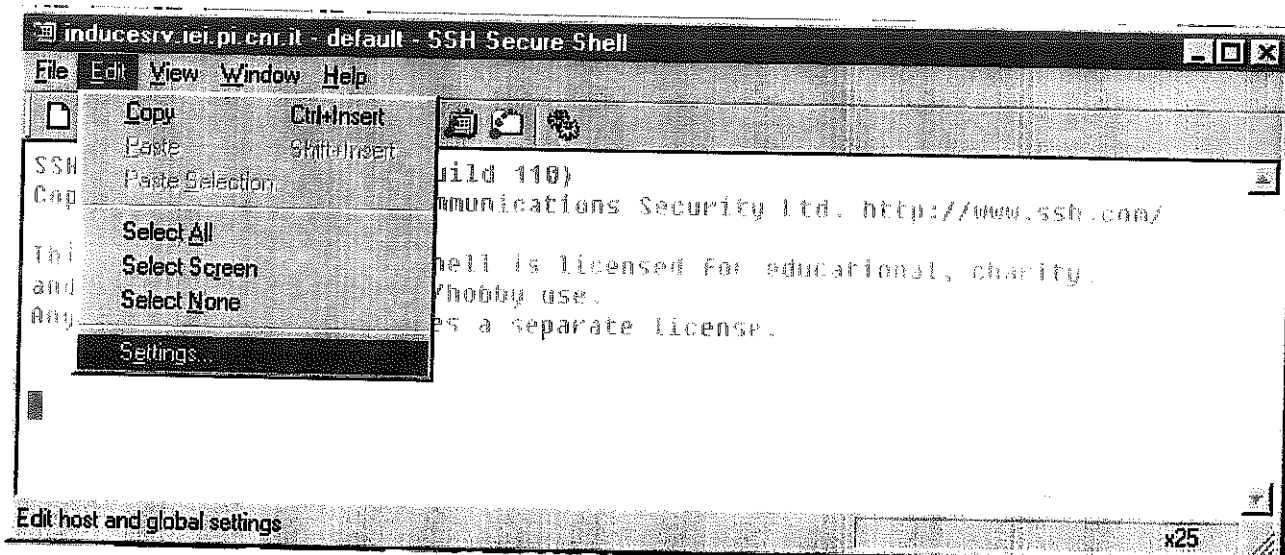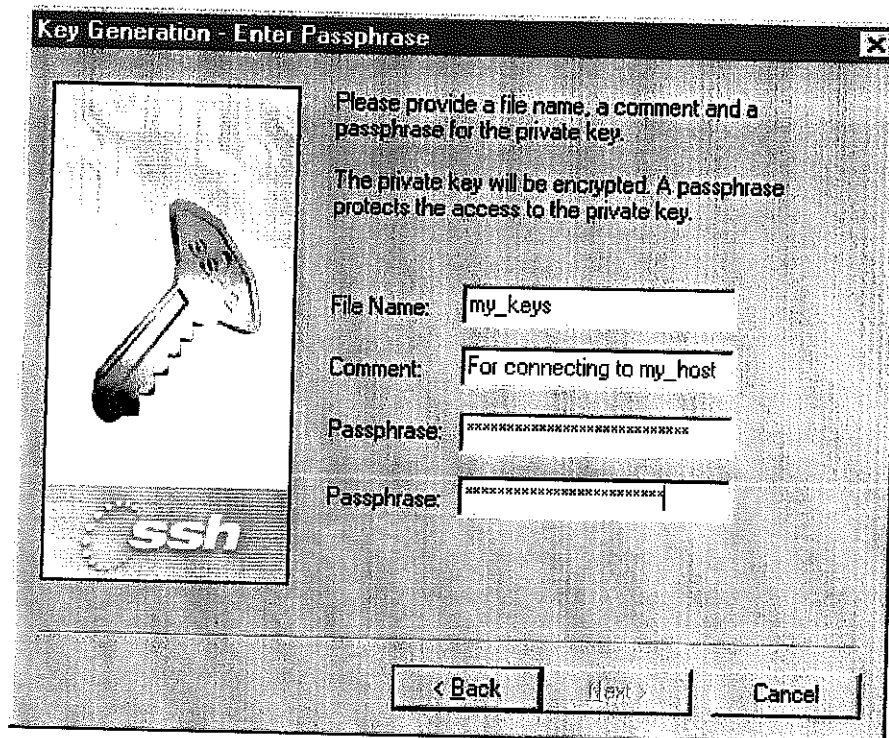
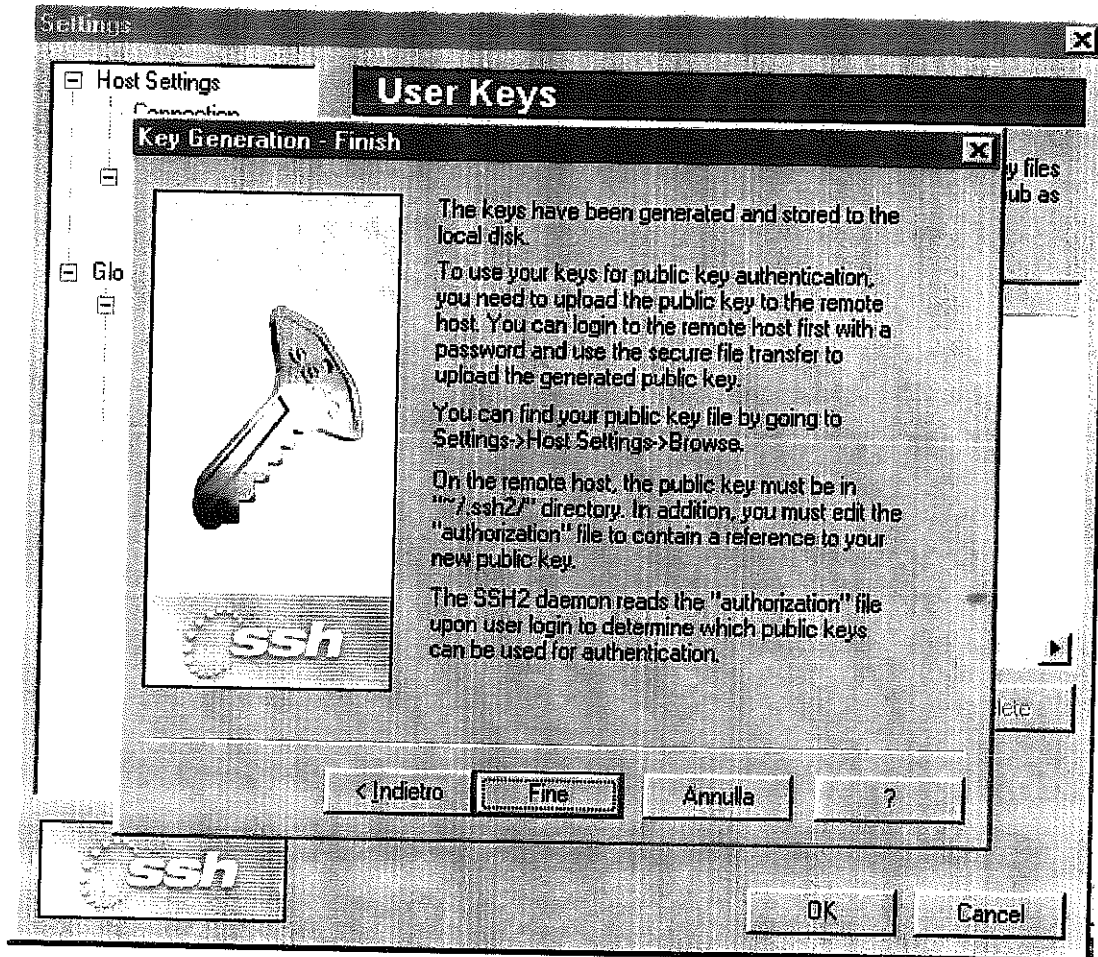| Date: *15.06.2000*	Reference N°:	**TR-2140-IEI-02**	Revision:	*1*	Pages:	5/12
					Annexes:	-
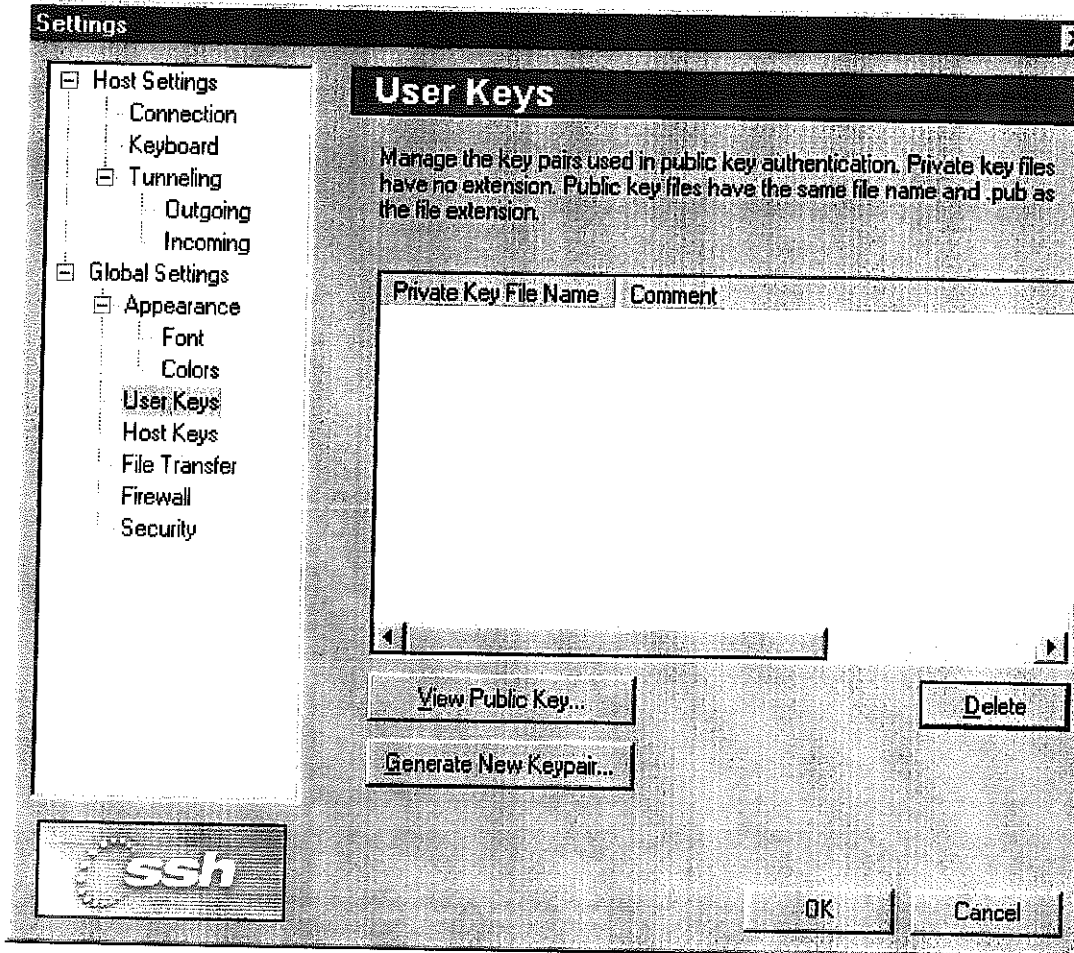
Now click the "Generate New KeyPair..." button.

Input a file name where your keys will be stored, e.g. "my_keys", and eventually write a comment in the proper field.
At this point, you must choose and write your password -*two times*- in *Passphrase*.

Click on the "Next >" button some times.

Project N° BE 97 - 4057
Contract N° BRPR - CT98 - 805

Date: 15.06.2000	Reference N°:	TR-2140-IEI-02	Revision:	1	Pages:	7/12
					Annexes:	-

At the end of this procedure you can connect to the INDUCE site.

Project N° BE 97 - 4057
Contract N° BRPR - CT98 - 805

| Date: *15.06.2000* | Reference N°: | **TR-2140-IEI-02** | Revision: | *1* | Pages: | 8/12 |
| | | | | | Annexes: | - |

The First Connection
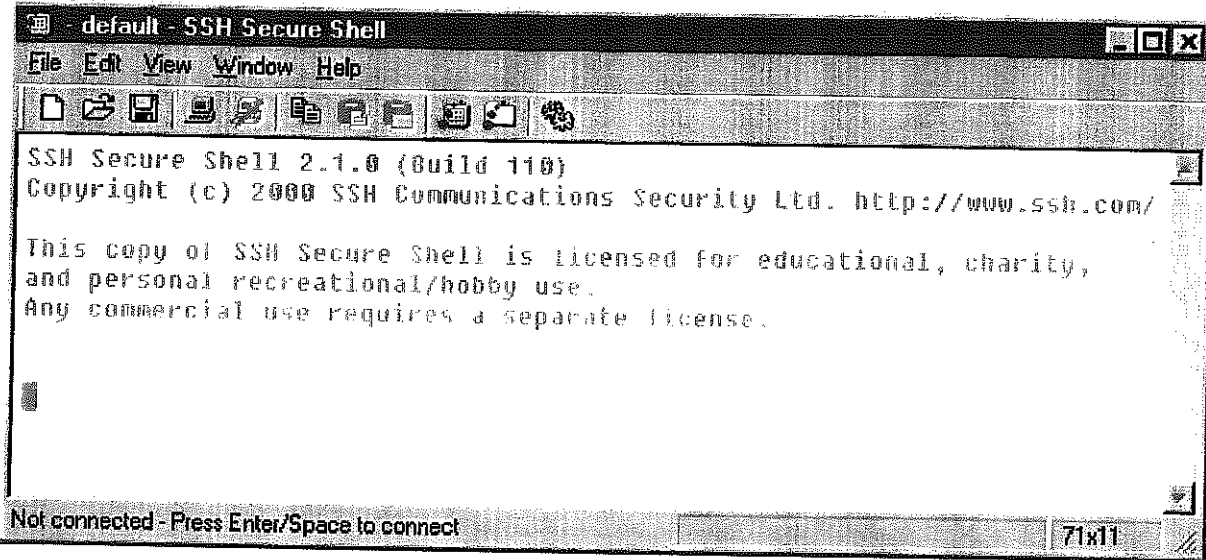
Choose the "Connect" voice from the "File" Menu
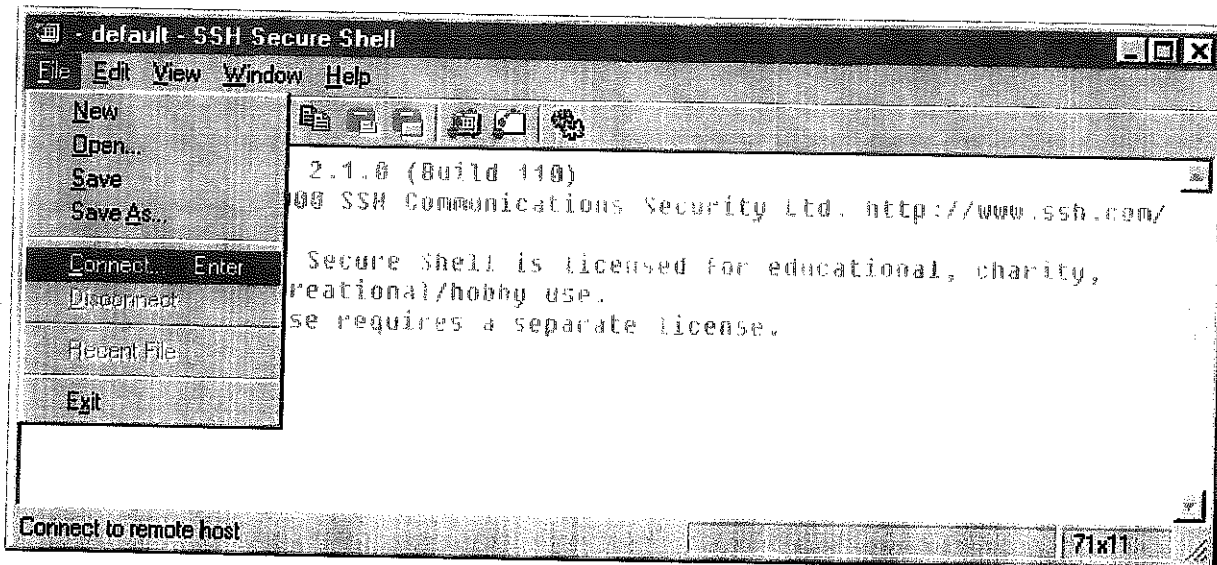
After having received some information, input (see next figure)
1) the name of the computer, that is inducesrv.iei.pi.cnr.it, then
2) 2) your **account** and
3) 3) your **password.**

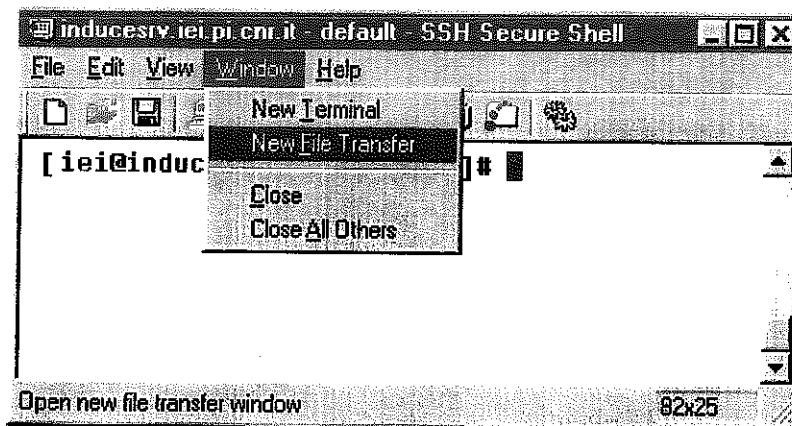| Date: *15.06.2000*	Reference N°: **TR-2140-IEI-02**	Revision:	*1*	Pages:	9/12
				Annexes:	-
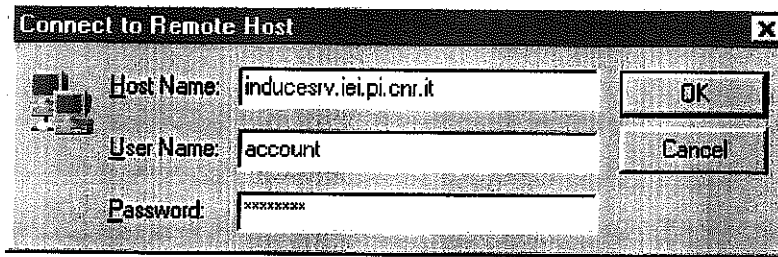
Once connected, it is necessary <u>to exchange your public key with the public key of the host</u> you are connected to: to this way, simply choose *yes* in the window displayed.
This procedure is requested only the first time the connection to the site is activated.
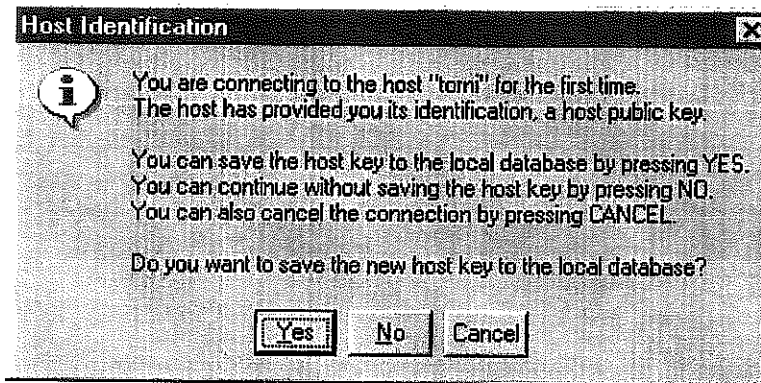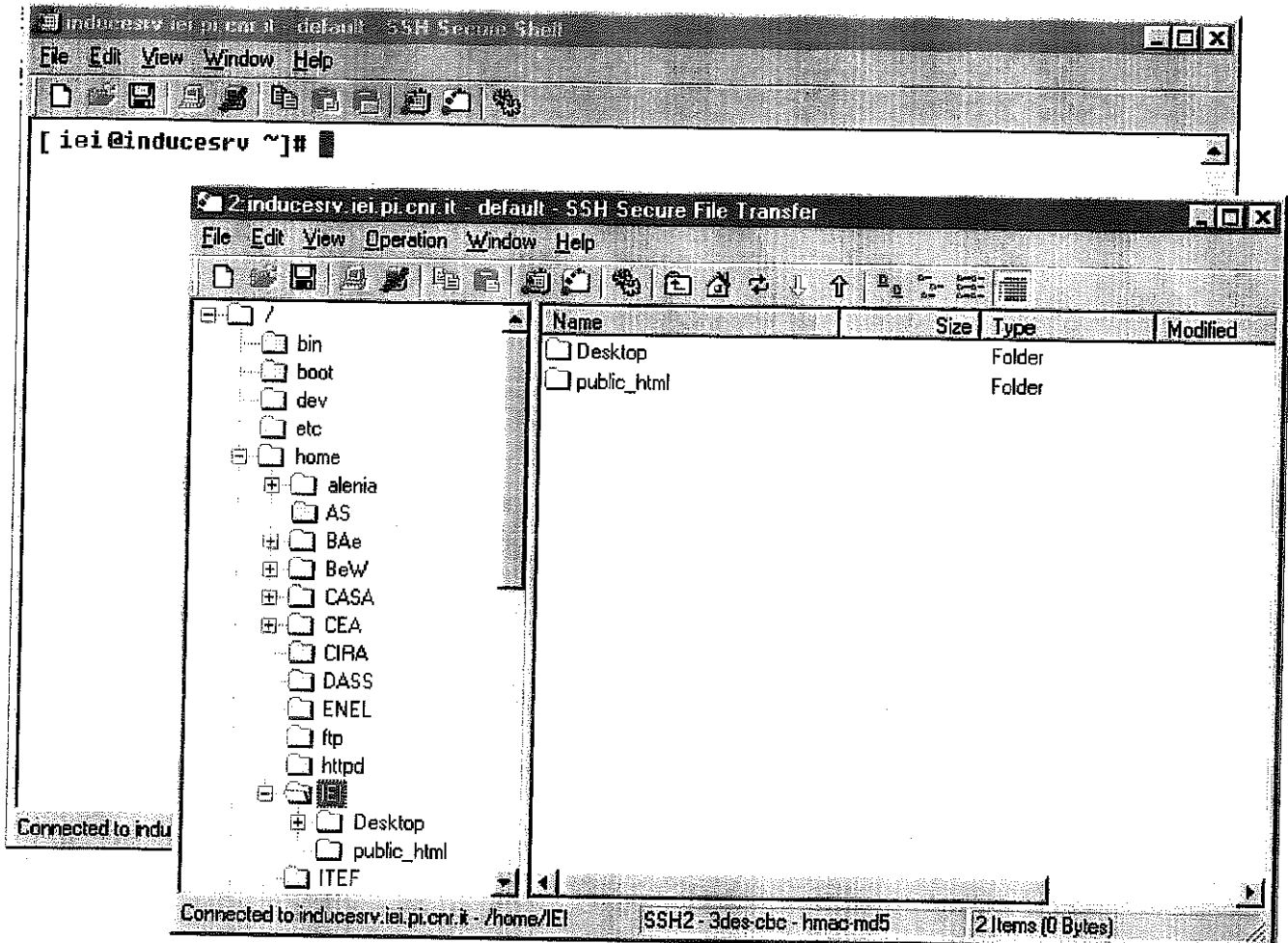

Steps for Writing in a Secure Way

In order to write information onto the site, select "New File Transfer" from the "window" menu.

Date: *15.06.2000*	Reference N°:	**TR-2140-IEI-02**	Revision:	*1*	Pages:	10/12
					Annexes:	-

At this point, drag and drop any file from your computer to your folder in the INDUCE site located on the right side of the "SSH Secure File Transfer" window.

In particular, you can drag the file from your computer directory and drop it in the public_html directory of the server; in this way, you can see the information using your web browser, connecting to your private area.

In the following two figures an example is shown where a file, called 'schema1.gif', is moved from our personal computer to the INDUCE site.

Date: *15.06.2000*	Reference N°:	**TR-2140-IEI-02**	**Revision:**	*1*	**Pages:**	11/12
					Annexes:	-

Date: *15.06.2000*	Reference N°:	**TR-2140-IEI-02**	Revision:	*1*	Pages:	12/12
					Annexes:	-

Steps for Reading in a secure way

Getting a file from INDUCE site requires to execute the inverse procedure, or to click the file on the "SSH Secure File Transfer" window and then to drag and drop it on the folder on your computer.

End of Session

At the end of the overall procedure, choose "Disconnect" from the "File" menu in all the windows opened (probably two, *ssh shell* and *file transfer*).

Sharing information with other INDUCE Partners

Sharing information with other partners needs firstly to inform the INDUCE Web-Administrator, via an email; he will transfer the specified file(s) in the directory named "common", located in the directory ".." (i.e., the parent directory)