

R-E-System

R-E-S V2.0

Characteristics of the “R-E-S V2.0”

“R-E-S V2.0” enables the encoding of all data, with absolutely the highest possible security. The coding is based on our own algorithm (**RFC-A/S**) which, when compared with all existing programs, is substantially stronger and materially faster.

The program is held on a USB key and when required, is connected to the computer. A major security feature is that the program limits activation to only that particular connection between the specific USB key and the computer upon which it was originally installed. Thus the integrity of the encoding and decoding procedure is assured.

Only the owner of the “R-E-S V2.0” can encode or decode files by the inputting of a password (1-64 characters).

Advantages of “R-E-S V2.0” compared with other encryption programs can be summarised as:

1. Strong encryption by use of our own **RFC-S** algorithm.
2. Key length of **4096-bit**.
3. Simple to install and operate.
4. “R-E-S V2.0” permits the normal encrypting of data on the computer (with if desired, a completely separate password for each individual document).
5. You can transmit such encrypted files via a Mail Server (or CD, Disc, USB etc.) with the exchange of public keys via the “**Diffie-Hellman**” method secured by our own **RFC-A** algorithm of **16,384-bit**.
6. No necessity to copy or otherwise manipulate the data to protect the original file format.
7. Encrypting of the data is carried out at the original file location.
8. Extreme security is assured by authentication protocols on the computer as well as the physical USB mass storage device and a separate **password**, plus an additional password can, if desired, be generated for any particular “**User Group**”.
9. All data encrypted is transparent and leaves no trace whatsoever on the computer.
10. The algorithm **RFC-A** and **RFC-S** has **absolutely no Backdoors**.

Should the USB key be lost or stolen, no potential exists for anyone else to access the encrypted data.

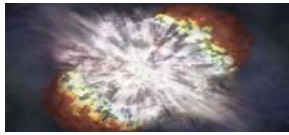
The passive security of the encrypted data (**at 4,096-bit**) is assured by the strength of the algorithm which has proved totally resistant to all mathematical attack methods. This algorithm was developed primarily for military cryptographic deployment, where ease of use, maximum security and speed of the ciphering and deciphering processes is paramount.

Anti-Virus Programs

No known problems exist with standard anti-virus programs and “R-E-S V2.0” with all files retaining their original format.

Firewall Programs

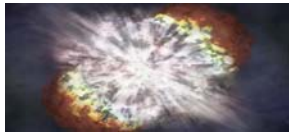
No known problems exist with standard Firewall programs and “R-E-S V2.0”.



R-E-System

Index

<u>1</u>	<u>INSTALLATION INSTRUCTIONS FOR THE „R-E-S V2.0“</u>	<u>3</u>
<u>2</u>	<u>“TOKEN PASSWORD” AND “KEY ID“ INSTALL INSTRUCTIONS FOR „R-E-S V2.0“</u>	<u>4</u>
2.1	GENERATE A PERSONAL “TOKEN PASSWORD AND PIN“:	5
<u>3</u>	<u>STARTING THE PROGRAM „R-E-S V2.0“</u>	<u>6</u>
3.1	AFTER GENERATE AND SAVE THE PASSWORD, START THE PROGRAM AS FOLLOWS:...	6
3.2	ADDITIONAL OPTIONS:	7
<u>4</u>	<u>SHORT FORM INSTRUCTIONS FOR „R-E-S V2.0“</u>	<u>7</u>
4.1	“PRIVATE KEY“	7
4.2	“AUTO PUBLIC KEY“ WITH OPTIONAL “SUB GROUP CODE”	7
4.3	“M-EDITOR”	8
4.4	GENERATION OF YOUR “PUBLIC KEY“ FOR OTHER USERS:	8
4.5	“PUBLIC KEY“	9
<u>5</u>	<u>KEY IDENTIFICATION</u>	<u>9</u>
<u>6</u>	<u>ACTIVATION OF LICENCE:</u>	<u>10</u>
<u>7</u>	<u>R-E-S SYSTEM LICENSE</u>	<u>10</u>



R-E-System

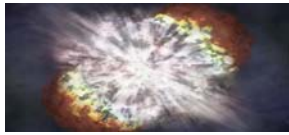
1 Installation instructions for the „R-E-S V2.0”

1. Connect a USB-Key to the computer.
2. Save the files **WindowLibarysSetup.exe**, **RESv20.exe** and **sRESv20.exe** to one USB key **(individually - not into a folder)**.
3. Execute the file "**WindowLibarysSetup.exe**" from the USB key.
4. Select the Language to use during the installation.
5. Confirm the input with "**OK**".
6. The installation window "**Welcome**" will open.
7. Confirm the input with "**Next**".
8. The installation window "**License Agreement**" will open.
9. Read the licence contract and confirm with "**I accept the agreement**".
10. Confirm the input with "**Next**".
11. The installation window "**Ready to Install**" will open.
12. Confirm the input with "**Install**".
13. The installation window "**Completing**" will open.
14. Click "**Finish**" to exit Setup.
15. Finally remove the USB key, close all open programs and restart your computer.
16. After you have restarted the computer, connect the USB key again and start the encoding program **R-E-S V2.0** with a **double-click on the file sRESv20.exe**
17. Now enter your chosen token passwords and PIN.
In the top on right-hand side (in the Yellow window), you can now enter the personal "**ID Code**" for your "**Key Identification**" (up to 16 characters). Click on the icon "»" and it will now open a different numerical window with which you can still expand the "**ID Code**". Click with the right mouse button on the number combination to enable it (white letters in black box). If you do not enable the numerical window, the program automatically creates a standard "**Code**" for this "**ID Code**". (This "**ID Code**" and the enabling number must be communicated to every person with whom you exchange any data under "**Auto Public Key**" and "**M-Editor**" (see "**Key ID Diagram. pdf**").
18. Now you can start to encrypt or decrypt files on the hard drive or, on removable flash drives.

Note: It is important that the program files (as in point number 2, above) be saved individually in a directory – **NOT IN A FOLDER** - **This critical.**

Do not delete the files: WindowLibarysSetup.exe, RESv20.exe and sRESv20.exe, from your USB-Key.

We recommend that you make a backup of the files and store in a secure location.



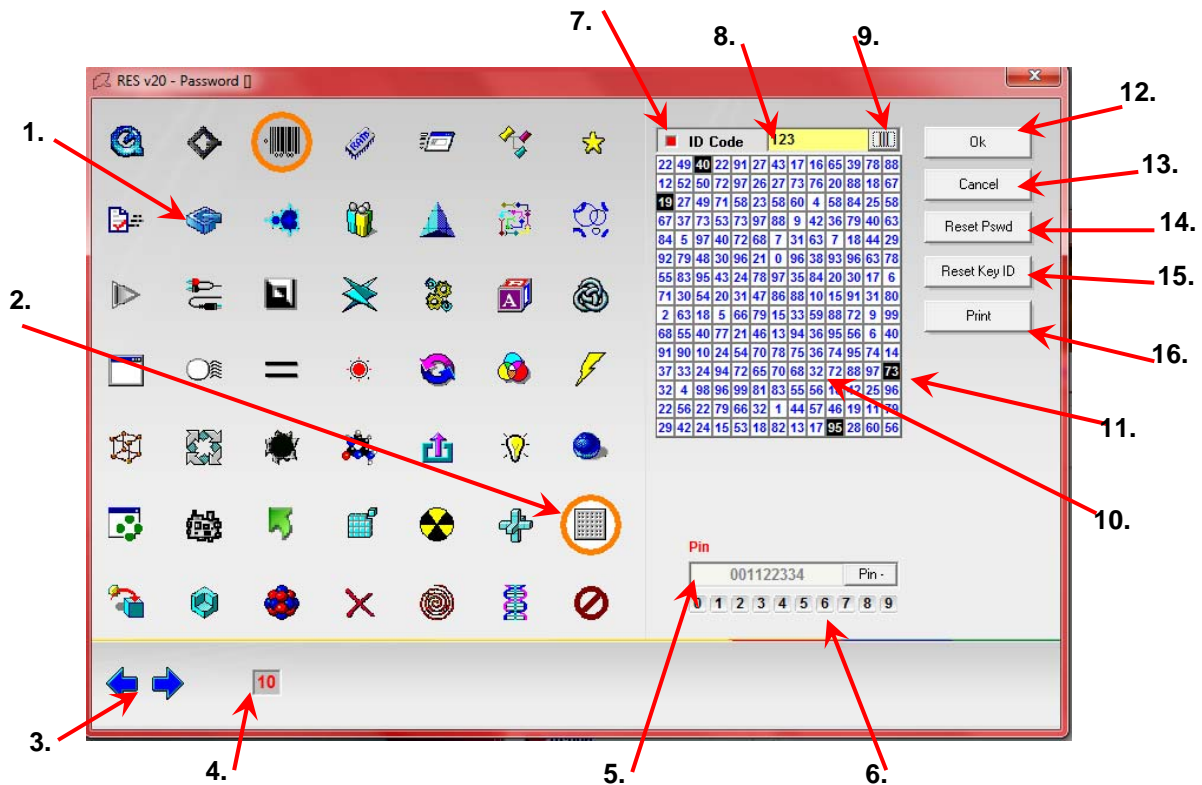
R-E-System

“Token Password” and “Key ID“ Install Instructions For “R-E-S V2.0”

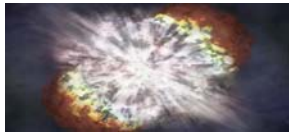
1. Connect the USB-Key to the computer.
2. Double-click on the file **sRESv20.exe**.

It opens the password window and you can now **generate your personal password!**

This password stores (automatically and encrypted) all your personal preferences and the **"Key Identification"** in different registers on the PC. There is no residual data stored on the USB stick.



1. Password image
2. Active Password image
3. Image search button
4. Countdown for the password input
5. Pin code
6. Pin code button
7. Key Identification control (red=inactive, green=active)
8. ID Code
9. ">>" open the numerical window of ID Code
10. Inactive numerical window
11. Active numerical window
12. OK button (to start the program)
13. "Cancel" button
14. "Reset Password" button
15. "Reset Key Identification" button
16. Print "Key Identification"

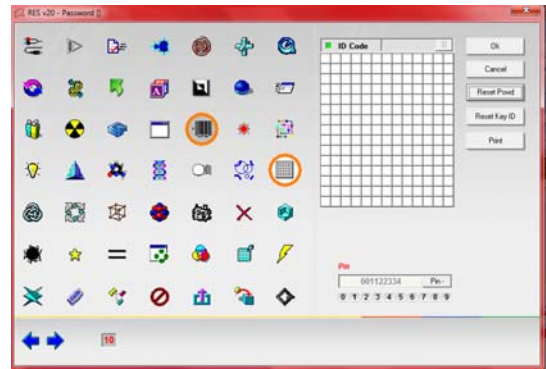
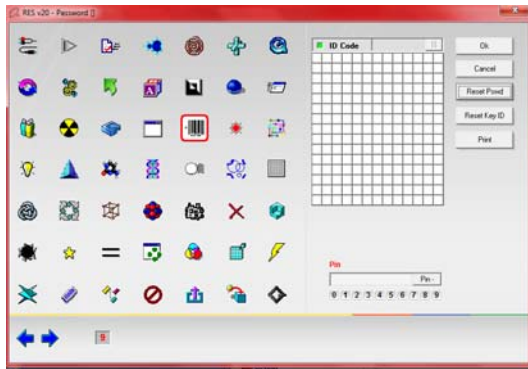


R-E-System

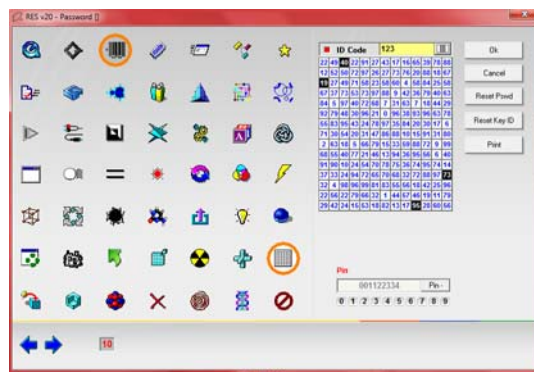
1.1 Generate a personal "Token password and Pin":

When you start „R-E-S V2.0“ the first time, you have to generate a personal password for the program:

1. To generate the "Token password" you must first select two of the 49 images.
2. Click on the first image of your choice (which activates it displayed in a white background with a red square frame).



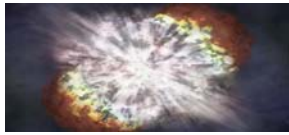
3. Now move this image onto the second image of your choice by dragging with the mouse.
4. In the window "Pin" on the right side enter your personal Pin.
5. In the top on right-hand side (in the Yellow window), you can now enter the personal "ID Code" for your „Key Identification“ (up to 16 characters). Click on the icon "»" and it will now open the different numerical window with which you can still expand the "ID Code". With the right mouse button Click on the number combination to enable it (white letters in black box). If you do not enable the numerical window, the program will automatically create a standard but equally secure "Code" for this "ID Code".



This "ID Code" and the enabling number must be communicated to all the people with whom you exchange any data under "Auto Public Key" (see "Key ID Diagram.pdf").

Note: To use "Auto Public Key" with other users, they all must have the same "Key Identification". "Auto Public Key" is always with the "Key Identification", if you switch your "Key Identification" you can no longer open encrypted documents.

6. Confirm the "Password" and "Key ID" with a click on the "OK" button.

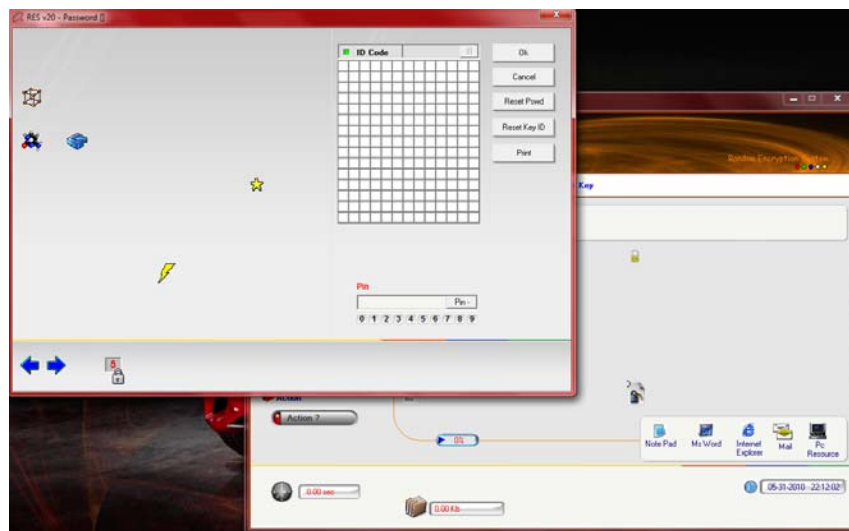


R-E-System

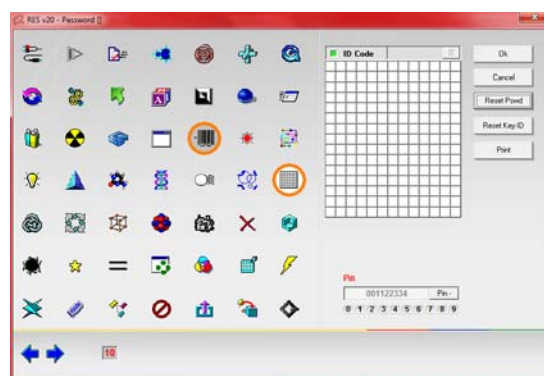
2 Starting The Program „R-E-S V2.0”

2.1 After generate and save the password, start the program as follows:

1. Connect the USB-Key to the computer.
2. Double-click on the file **sRESv20.exe**.



3. The password window now opens automatically. Unlike in the generation steps, you will only see 5 of the 49 images.
4. Using the back and forward arrow buttons, select the first image of your token password.
5. Enable the first image (using the mouse button) which will appear in a rectangular red frame with a white background.
6. Again using the back and forward buttons, select the second image of your token password.
7. Next, click on the first image and drag it onto the second image of your selection.
8. The images now appear in a round orange frame the first having a grey background and the second with a white background.



9. Enter your "Pin" (click with the mouse button on the number) exactly the same as when you generated the password.
10. On the right of "Key Identification" (top right) you will see a pale green box indicating that your personal "ID code" (with all possible additional number combinations) is active.
11. Confirm your entries with the "OK" button.
12. The program will now be automatically enabled as the "Key Identification".

You can now start encoding and decoding your documents.



R-E-System

2.2 Additional options:

1. With the "**Cancel**" button, you can delete any errors.
2. With the "**Reset Password**" button you can erase the current password.
3. With the "**Reset Key Identification**" button you can erase the current "Key Identification".

Warning: Remember to Decrypt all your old files previously encrypted with any old password or old Key ID before you confirm the reset function.

4. Print "**Key Identification**": Print your "Key ID code" (keep this in a safe place)

Note:

The **Password** is uniquely connected with all the documents that have been encoded with "**Private Key**", however, the "**Key Identification**" is not active for these documents.

Any documents that have been encoded with "**Auto Public Key**" and any "**M-Editor**" text are always connected with the "**Key Identification**", and you can at any time change your password without in any way altering the "**Key Identification**".

3 Short Form Instructions For „R-E-S V2.0”

1. Connect the USB-Key to the computer.
2. Double-click on the file **sRESv20.exe**.
3. Now enter your chosen token passwords and Pin and you can start to encrypt or decrypt files.

3.1 “Private Key”

Encoding with “**Private Key**”:

1. Select under “**Setting**” the option “**Private Key**”.
2. Select the document in the data window (left-hand side) that you wish to encode.
3. Encode the document with a click on the **Crypt** button.

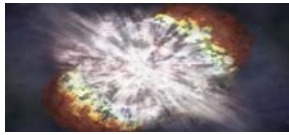
Decoding with “**Private Key**”:

1. Select under “**Setting**” the option “**Private Key**”.
2. Select the document (**Black Text**) in the data window (right-hand side) that you wish to decode.
3. Decode the document with a click on the **DeCrypt** button.

3.2 “Auto Public Key” with optional “Sub Group Code”

Encoding with “**Auto Public Key**” with optional “**Sub Group Code**”:

1. Select under “**Setting**” the option “**Auto Public Key**”.
2. If you want an optional “**Sub Group Code**”, enter the code (right-hand side).
3. Select the document in the data window (left-hand side) that you wish to encode.
4. Encode the document with a click on the **Crypt** button.



R-E-System

Decoding with “**Auto Public Key**“ with optional “**Sub Group Code**“:

1. Select under “**Setting**“ the option “**Auto Public Key**“.
2. If you get a “**Sub Group Code**“ code, enter the code (right-hand side).
3. Select the document (**Blue Text**) in the data window (right-hand side) that you want to decode.
4. Decode the document with a click on the **DeCrypt** button.

Note: To use “**Auto Public Key**“ with other users, they all must have the same “**Key Identification**“. “**Auto Public Key**“ is always with the “**Key Identification**“, if you switch your “**Key Identification**“ you will not be able to open the documents. For simplicity and ease of use, we recommend that unless hierarchical groups are required, you use the simple “**Auto Public key**“ option without the “**Sub Group Code**“ for general work.

3.3 “M-Editor”

Encoding and decoding of short message (written solely in the memory) only under “**Auto Public Key**“ and “**Auto Public Key**“ with “**Sub Group Code**“:

Encoding with “**M-Editor**“:

1. Select under “**Setting**“ the option “**Auto Public Key**“.
2. If you get a “**Sub Group Code**“ code, enter the code (right-hand side).
3. Select from the list on the left-hand-side the option “**M-Editor**“.
4. Then simply write your text under “**Plain Text**“ (top white window titled “Plain Text”).
5. Encode the text with a click on the above **Crypt Msg** button which displays the encrypted message in the lower blue window.
6. Click on “**Copy**“ alongside the blue window which copies the message to the clipboard and insert (by right clicking Paste with the mouse) the “**Encrypted Message**“ into an e-mail.
7. Send this e-mail to the decided people - they all must have the same “**Key Identification**“.

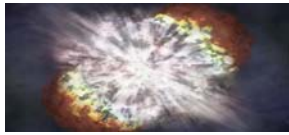
Decoding with “**M-Editor**“:

1. From an incoming e-mail with M-Editor content in the body, copy the entire encryption display from -->**BEGIN-MSG** to <--**END-MSG** inclusive to the clipboard.
2. Select under “**Setting**“ the option “**Auto Public Key**“.
3. If you get a “**Sub Group Code**“ code, enter the code (right-hand side).
4. From the list on the left-hand side, select the option “**M-Editor**“.
5. Paste the Message into the lower blue window simply clicking on the **Paste** button.
6. The encrypted message is displayed in the blue window and by simply clicking on the **Decrypt Msg** opposite the upper white window, the message is displayed in plaintext.
7. You can read the message or, if desired, save it by highlighting, copying and pasting to Word and saving in the conventional manner.

Note: To use “**M-Editor**“ with other users, they all must have the same “**Key Identification**“. “**M-Editor**“ is always associated with the “**Key Identification**“, if you switch your “**Key Identification**“ you will not be able to open the encrypted message.

3.4 Generation of your “Public Key“ for other users:

1. Select under “**Setting**“ the option “**Public Key**“.
2. Click on “**Compute Key**“ to generate one “**Public Key**“.
3. Click on “**Copy**“ and insert the “**Public Key**“ into an e-mail.
4. Click on “**Cancel**“.
5. Send this e-mail to other Users who can now use this key for secure communications with you.



R-E-System

3.5 "Public Key"

Encoding with "Public Key" for other users:

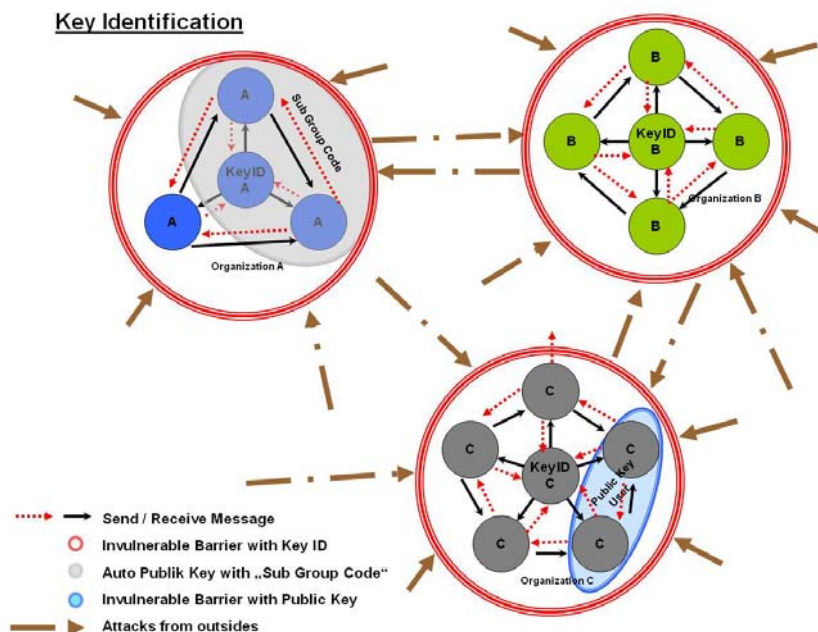
1. Select under "Setting" the option "Public Key".
2. Insert under "Public Key" the obtained "Public Key" with the "Paste" button, and confirm with "Setting".
3. Select the document you wish to encode from the data window (left-hand side).
4. Encode the document with a click on the **Crypt** button.
5. Now send this document to the person who gave you their "Public Key".

Note: The data that you encode with "Public Key" can only be decoded by the person that sent you their "Public Key" generated with his USB key; which means that even you cannot now decode this data.

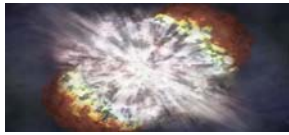
Decoding with "Public Key":

1. Select under "Setting" the option "Public Key (Decrypt Only)".
2. Select the document you wish to decode (**Red Text**) from the data window (right-hand side).
3. Decode the document with a click on the **DeCrypt** button.

4 Key Identification



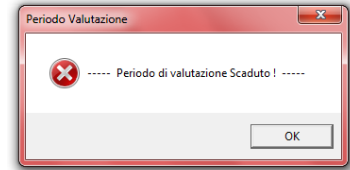
Note: To use "Auto Public Key", "Public Key" and "M-Editor" with other users, you must all have the same "Key Identification" (example: Key ID A).



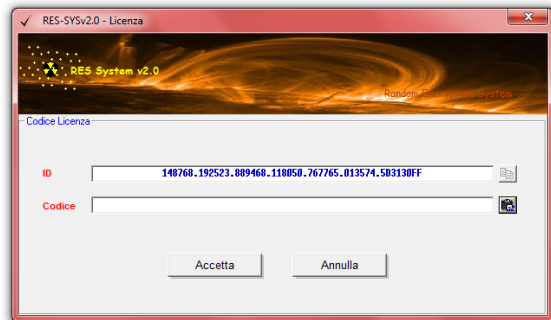
R-E-System

5 Activation of licence:

If the test license of „R-E-S V2.0” has expired, the window “Evaluation Period Expired” is displayed.

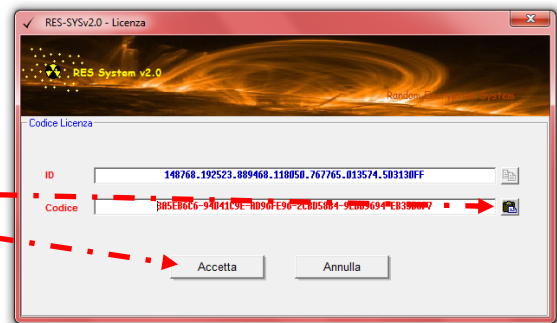


You must now click on the **OK** button to open the license activation window.



Copy the ID number and send it (via e-mail) and the payment to your reseller who will obtain your Licence number.

You will get your license via e-mail, and you should carefully copy such license number by highlighting it, “copying” and then “pasting” into the Licence window. Confirm the license number by clicking on the “Accept” button.



6 R-E-S V 2.0 License

Date:	
Name:	
First Name:	
Country:	
E-Mail:	
R-E-S-V 2.0 Licence ID:	
License:	
Bankcode:	

Please Ensure your licence information is kept in a safe place
R-E-S accepts no liability for any incident of theft, loss or other abuse of the program