Table of content

1 The RSA Software Token ................................................................. 2
  1.1 Using a RSA Secureid software token ........................................... 2
  1.2 How to get a RSA Secureid software token ..................................... 2
  1.3 How to troubleshoot your RSA software token ................................ 6
    1.3.1 The troubleshooting site ...................................................... 6
    1.3.2 Reset my PIN code ............................................................ 7
    1.3.3 I don’t have my token with me ............................................. 7
2 Accessing SSH (ssh.eurecom.fr) ......................................................... 7
3 The SSL VPN (https://vpn.eurecom.fr) ................................................ 8
  3.1 Usage ...................................................................................... 8
  3.2 Accessing the SIFI through the SSL VPN ...................................... 10
  3.3 Accessing your homedir and the teaching repository through the SSL VPN 11
1 The RSA Software Token

To connect yourself from outside to EURECOM internal services, you must use a RSA Secureid software token. The idea behind the RSA token is to prevent EURECOM from keylogers and too simple passwords. The RSA token is a software which computes a new “One Time Password” valid for one minute.

The software token can be install on one device only. You have the choice of this device (your smartphone, your laptop etc...). We recommend you to install software token on a SMARTPHONE since it is likely that you will have it always with you.

1.1 Using a RSA Secureid software token

We only use software token which, once you enter your personal secret (PIN code), generate a unique passcode valid during one minute. You have then to copy this passcode into the EURECOM application you want to access.

Example from a laptop:

1.2 How to get a RSA SecureId software token

Since the software token can be installed on one device only, you have the choice of this device (your smartphone, your laptop etc...). Again, we recommend you to install software token on a SMARTPHONE since it is likely that you will have it always with you. Please note that you should be able to read email on the device where you plan to install the software token since the activation will come by email.

Getting the software token to work requires 2 main actions : you should first install a software that you can download from the web, and second activate the token in that software (using an email we are going to send you). The different steps are :

1. **Choose the device** you want to use (IPhone, AndroidPhone, windows PC, Apple Mac etc...)

2. **download the software** (search for rsa software token) from a “store” related to the device (applestore, playstore, or from the RSA web site http://france.emc.com/security/rsa-securid/rsa-securid-software-authenticators.htm#!offres_pour_les_ordinateurs for mac and windows PCs, choose the 32 or 64 bits “Desktop Application with Software Token Automation” etc...).

3. **Install the software** on your device

4. **access the email** sent to you by IT service on the device (this email should include as a link your own personal token (link to a CT-KIP service) )

5. **Two cases** :
   1. **For smartphones, click on the correct link (android, iphone, blacberry, windowsphone)**
      - Smartphone : select the link corresponding to your hardware, open it using SecurID Software token and enter manually the code given in the mail.
2. For Laptops: choose “import from web” and copy the link for Laptops and the activation code into the RSA Token.

6. go to https://token.eurecom.fr to generate your personal PIN code: At this step, you will have to enter your login and your windows password. Since it is your first login onto the system, the server will ask you to choose 5 “security” questions (among 15) and give it the answers. The server may use these “security” questions to authenticate yourself when the primary authentication method results in a failed authentication. “Security” questions is a backup authentication method that requires users to answer questions in order to authenticate.

- go to https://token.eurecom.fr
- enter your User ID which is your EURECOM loginname (without @eurecom.fr)

Choose password
Enter your EURECOM windows password (into EURECOM domain)

Using the server for the first time, you’ve got to choose/answer 5 “security” questions. It is important to choose questions that you can answer without doubts, because the later on, when you will try to connect to it (for example for troubleshooting purposes), the server may ask some of these questions in order to verify that it is really you...
Click on the “Create PIN” link

The welcome page of token.eurecom.fr should indicate you if you've got a token without any PIN code: click on « create PIN »: the system generates a personal PIN code you’ll need to enter each time you want to use your token (DO NOT FORGET IT):
1.3 How to troubleshoot your RSA software token

1.3.1 The troubleshooting site

In addition to give you your PIN code, the web site https://token.eurecom.fr is dedicated to self-service tools for RSA tokens. It allows to initialize or re initialize your personal PIN code, unblock resources access when you’ve forgotten or lost your token ... . You first have to login as in the previous step (using EURECOM login and windows password)

Once logged on, you can access to tools made to unblock your external access authenticated by RSA. For that purpose you have to click on “troubleshoot” on your software token:

You then have two options :
- I forgot my PIN code will allow you to generate a new PIN code.
- I don’t have my token will give you a temporary “emergency token” which will have a limited validity (generally one day).
1.3.2 Reset my PIN code

Just click on the “I forgot my PIN” in the previous “troubleshoot your token” screen and click on “create PIN” :

![Change Your PIN](image)

1.3.3 I don’t have my token with me

Just click on “Token is temporarily unavailable or misplaced”. The system generates a temporary “Emergency Access Tokencode” to use instead of your token code. To use it, enter as passcode your PIN code FOLLOWED by this special “Emergency Access Tokencode” :

Passcode = Pincode + “Emergency Access Tokencode”

![Emergency Access](image)

2 Accessing SSH (ssh.eurecom.fr)

It is possible to access your data from outside using the EURECOM ssh server. For that purpose, you will need a ssh client to be installed on your PC (putty is an exemple). The client will allows you to “login” on a EURECOM computer (with a ssh client shell) transfer files (with the secure file transfert client). Using ssh requires you to have an RSA software token.

The EURECOM ssh server is ssh.eurecom.fr

Your login is your login name,
Your password is your RSA passcode (code generated by RSA software token)
3 The SSL VPN (https://vpn.eurecom.fr)

3.1 Usage

The VPN SSL solution offers a single centralized access point for accessing internal information from the outside. The main principle of such a solution is to offer a secured web portal which

- Authenticate each user
- Offer each user the internal access he’s authorized to.

The SSL VPN is supposed to work on windows (XP and seven), Linux and MacOS10. Please contact us in case of problem. (do not use chrome)

The EURECOM SSL VPN is a lightweight VPN. It does not require any user installation and thus does not require you to be administrator of the machine.

Use the SSL VPN (https://vpn.eurecom.fr) is only accessible using your login and RSA passcode. This requires you to have a RSA software token.

Here is a step by step guide of how to connect to the SSL VPN (a more detailed documentation is available on the EURECOM web at http://www.eurecom.fr/en/eurecom-tools):

   (Note: Browser Configuration: you must allow window pop-up to be able to use some applications supported by SSL VPN like the SIFI).
2. Fill ALL the 4 fields as follow and click logon:

<table>
<thead>
<tr>
<th>Group</th>
<th>Eurecom</th>
</tr>
</thead>
<tbody>
<tr>
<td>USERNAME</td>
<td>Your Eurecom Login</td>
</tr>
<tr>
<td>Windows Password</td>
<td>Your windows password</td>
</tr>
<tr>
<td>RSA PassCode</td>
<td>Your RSA password, this password is used to login into the VPN. It is a 8 digit number generated by your RSA secured software token once you’ve entered your personal PIN code (it is valid for one minute)</td>
</tr>
</tbody>
</table>

3. You can then see all the options available to you listed in 4 separated zones:
Please note that once you connect to an application, you should always be able to get back to this screen by clicking on the “home” icon that appears at the upper right corner of the window.
3.2 Accessing the SIFI through the SSL VPN

Please Note that some of the Eurecom sites requires **popup not to be blocked**. The SIFI is one of these sites, in that case, when you click on a tool that tries to open a popup (ie the pencil in the following screen), a message appears in the light yellow bar:

You then have to click on the message and authorize popup from that site. Note that you may also authorize all the popup from Eurecom.fr in the tools menu of “internet explorer”.

![Image of the SIFI access through SSL VPN](image-url)
3.3 Accessing your homedir and the teaching repository through the SSL VPN

When you select one of the file bookmarks, you have access to the corresponding files using the following web browsing interface. You can then browse copy and paste files...

If you are using internet explorer you can select the “web folder” icon (see below on the left), and you will be able to browse your file as if you were using windows explorer (this will prompt you for a “security Alert” that you will have to accept (see below on the right).

You will then see your files as if you were using explorer, be cautious that it is just a flavor of explorer, and don’t do too complex operations using that interface.