For this Technical Tip, I've used a 3rd Party product, called LUNA 2. More detailed information on LUNA 2 could be retrieved via www.chrysalis-its.com. If you need a contact name within Chrysalis-ITS, please send an email to rainer@bemsel.com and I'll get somebody sending you product info and where to get an evaluation kit or where to buy the product. As the VPN Client, I have used TimeStep's PERMIT/Client.

Without Luna 2, Entelligence uses an EPF file to store users profiles on a floppy disk or a hard drive. Although profiles are hashed with a password, and certificates are encrypted and signed by the CA, this is not a secure method for storing your Public Decryption Key, or Signing Key Certificates.
The Luna 2 token provides a secure method for storing your keys and certificates that seamlessly ties into the Entrust/Entelligence application. Whether you are setting up a new Entrust user account or wish to move an existing profile to a Luna 2 token, the processes are straightforward and are described in this document.

Installing the Hardware

First, I describe how I did the hardware and driver installation to make Luna 2 ready to use. I've used a card reader, which is controlled to the computer's PCI bus. I recommend using the Chrysalis-ITS Luna Dock reader.

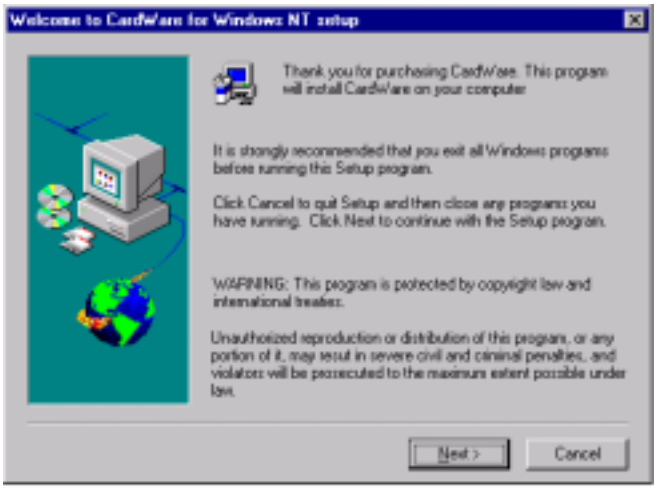
Installing the Driver

Start the computer

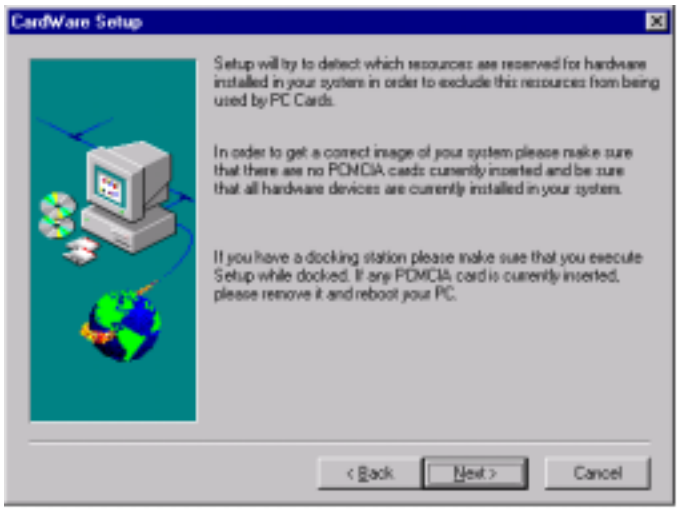
Login to Windows NT as Administrator, or as a user with admin privileges

After the startup and login process is complete, insert the drivers CD, which is bundled with the hardware.

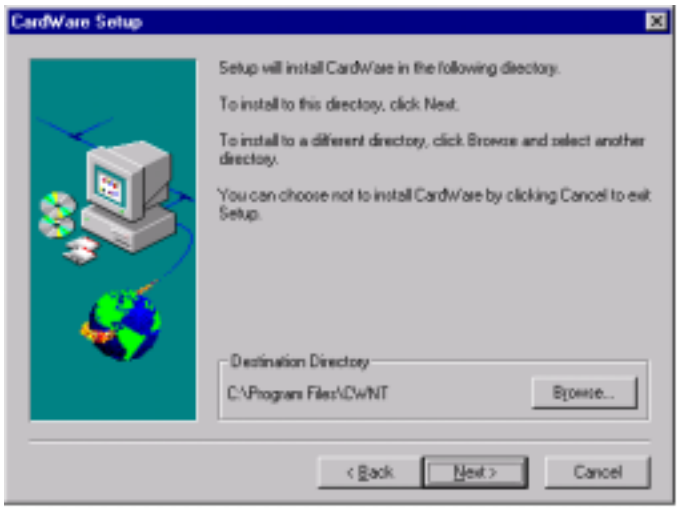
Install the CardWare software by running Setup.exe under the \Cardware\Disk1 directory on the CD



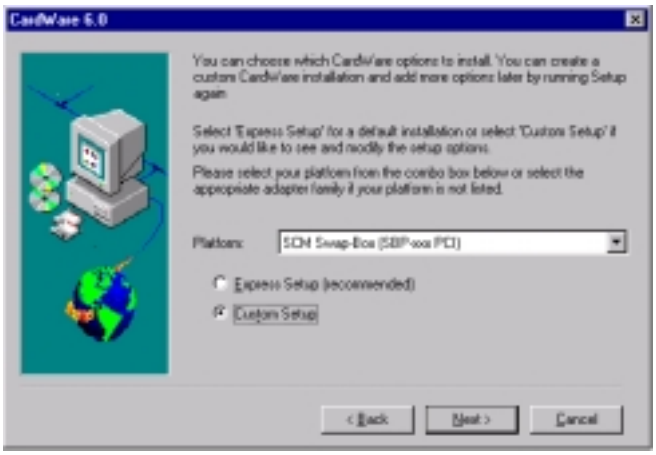
The Welcome screen appears. Click on **NEXT**



You should have the Dock Reader installed, however if there are any PCMCIA cards inserted, please remove them. Click on **NEXT**

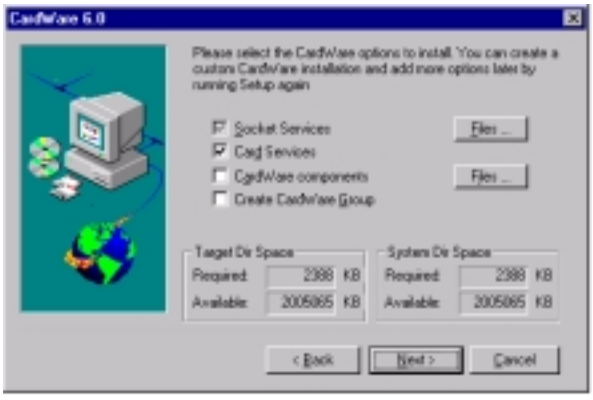


Accept the default directory and click on **NEXT**



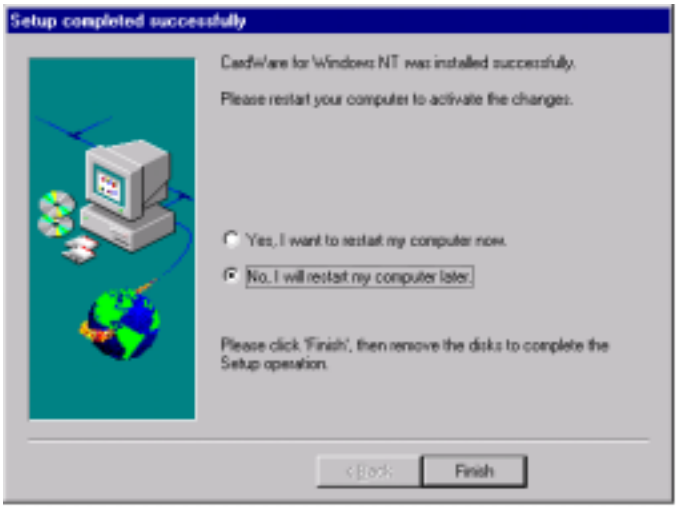
Change to Custom setup and choose the default setting ***SCM Swap-Box*** as the platform.

A new hardware profile will be created, where you can choose NT's startup parameters



Deselect ***CardWare components*** and ***Create CardWare Group***

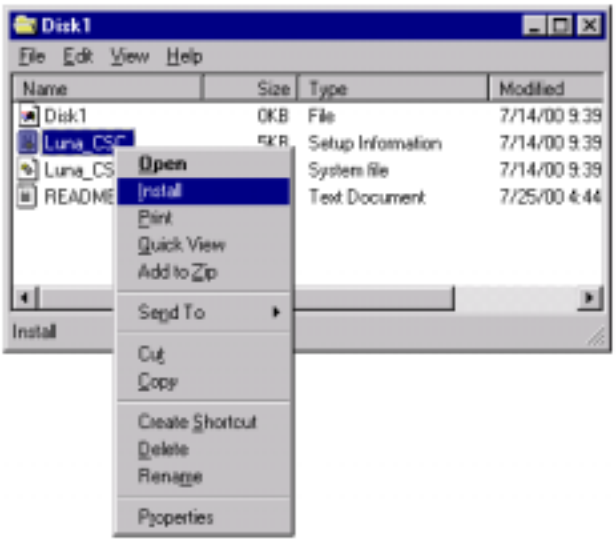
The "CardWare Load Control" dialog appears. Click **'Next'** button
(A progress bar appears and the installation is going to be finished in few moments)



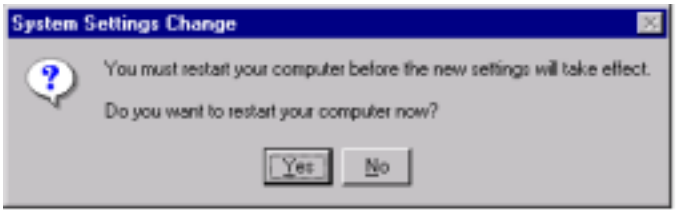
Select **No** I will restart my computer later.' Click **Finish**

Apply the Luna Card Services Client Driver patch files

- Insert CD-Rom labeled Service Pack #1



Right-click on the "Luna_CSC.inf" file and select "**Install**". A system change settings window appears



Select ***'yes'*** I wish to reboot my computer now

When done with installation, reboot the system and the reader is now ready. You'll see a new hardware profile, which says "**TouchStone CardWare profile**". This profile has been added during the installation process. Choose this profile to start Windows NT.

Installing Luna 2 with Entrust on Windows NT

I am using Windows NT 4.0 Server, which also acts as my Registration

Log into Windows NT as "Administrator" or as a user with administrator privileges
Ensure that you do not have any LUNA product installed before using the setup disk. When having any LUNA product installed, uninstall them and remove any directories named LUNA. Under winnt/System32/drivers, remove any files named

`luna_nt.sys` or `luna_csc.sys`

You should also manually remove the file: *c:\winnt\crystoki.ini*, which is not automatically removed by “Add/Remove programs

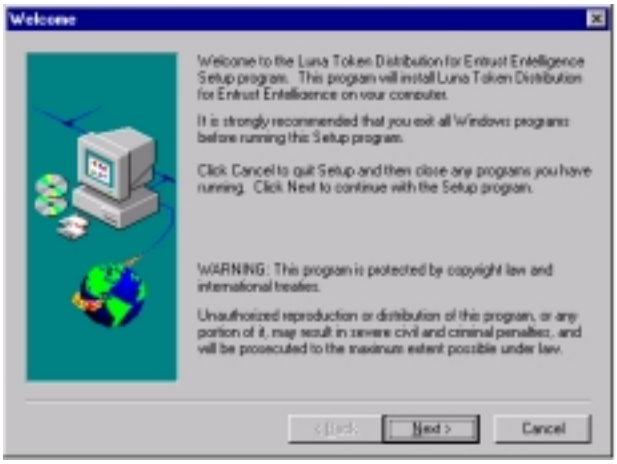
1. Before you start with this installation, you should have Entrust Certificate Authority installed.
   Following link outlines the steps to install Entrust 5.0 on Windows NT

   http://www.bemsel.com/TechTip/RB_i500_Entrust5_v1.2.pdf
   or
   http://www.bemsel.com/omnitip_collection/i500_Entrust5_v1.2.pdf

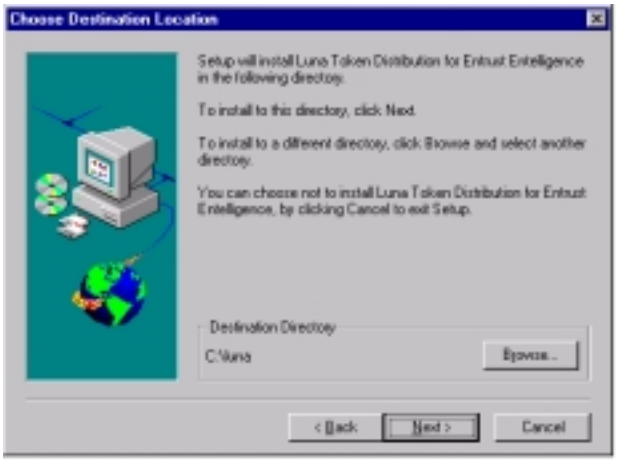
2. Install Luna 2 library and driver software form the Luna 2 CD.

   Insert the “Luna PKI Enterprise Systems CD (Luna 2 for Entrust/Entelligence 5.0.2) in your CD drive. If Auto run is working, a dialog box appears. If you have disabled Auto run on your system, click Start/Run and then type:

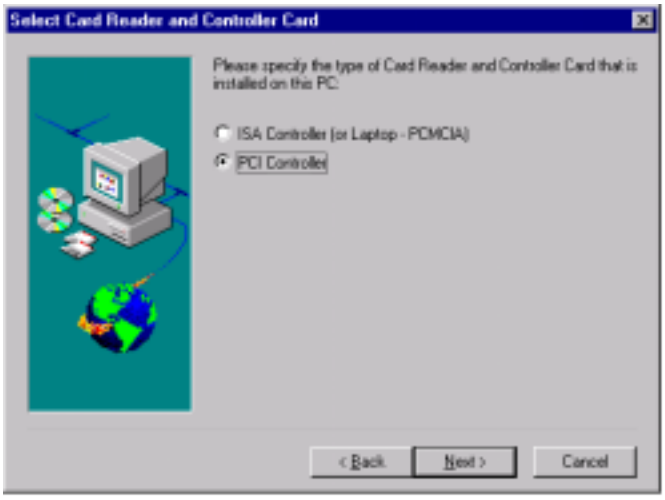
   ```
   <driveletter of CD ROM> \windows\lunasetup.exe
   ```



Click on NEXT



Accept the default location and click **NEXT**



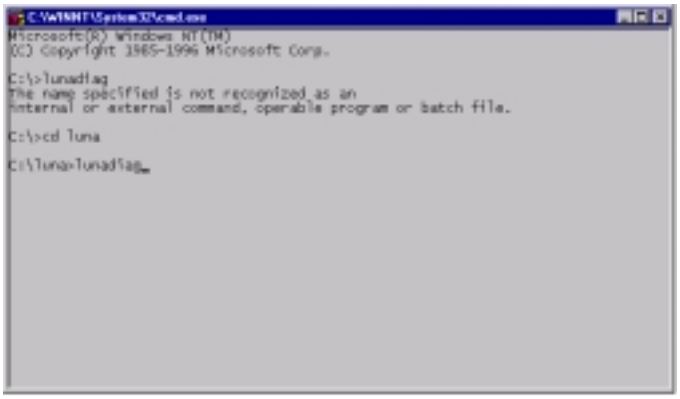
I've done two different scenarios, where the first installation run on the Entrust Certificate Authority to be able for creating a profile locally and distribute to each individual clients. The next scenario, I'll describe later in this document with be a client for online certificate enrollment on a Notebook. Depending on you PC, choose the proper selection.
(A progress bar appears)

When finished, a restart window appears. Do a reboot after installation has been completed and re-logon as administrator.

To confirm a proper installation, insert a token into a reader slot and run lunadiag.exe from the \LUNA directory.

Open a command box (DOS) and change into c:\luna. Execute the command

```
C:\luna\lunadiag.exe
```



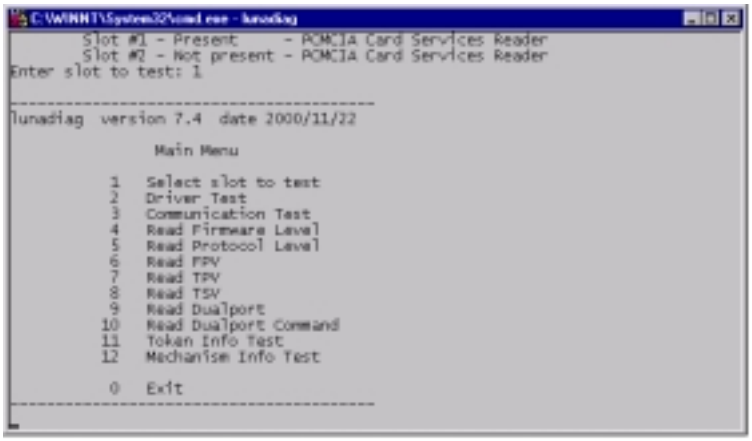
Choose the proper slot, for example

```
C:\luna\lunadiag.exe
Lunadiag version 7.4   date 2000/11/22
Detecting Luna devices …
Detection complete

Slots available:
      Slot #1 – Present       - PCMCIA Card Services Reader
      Slot #2 – Not present   - PCMCIA Card Services Reader
```

Press the number of the slot, where you see “Present”.

Do a Driver Test and Communication Test. When getting “Test passed”, everything is just fine.



Press 2 for Driver Test:

A successful test looks like that:

```
[Testing slot 1]
Luna drivers      (c:\WINNT\System32\Drivers\Luna_NT.sys) detected …
File name         : c:\WINNT\System32\Drivers\Luna_NT.sys
File size         : 65380 bytes
File time         :Mon Aug 13 19:27:09 2001
```

Press 3 for Communication Test

A successful test looks like that:

```
[Testing slot 1]
Test passed.
```

Verify, that Luna 2 settings has been added into the ***entrust.ini***, which remains in c:\winnt. You also need to add this line to any other entrust.ini, when having LUNA 2 installed on a Certificate Authority, for example in the *C:\Program Files\entrust\entrust RA* - Directory. You may better do a file search. I've found four of them, but didn't modify the one in my backup directory.

Find in the settings section, that CrystokiLibraryNT has the proper pointer.

```
[EntrustSettings]
CrystokiLibraryNT=c:\Luna\crysto32.dll
```

Note*: You may have a different location, when having Luna installed under Program Files*

IMPORTANT: When using a notebook with another PCMCIA card inserted, please read the README file in the directory c:\luna\ethcdfix, before you continues

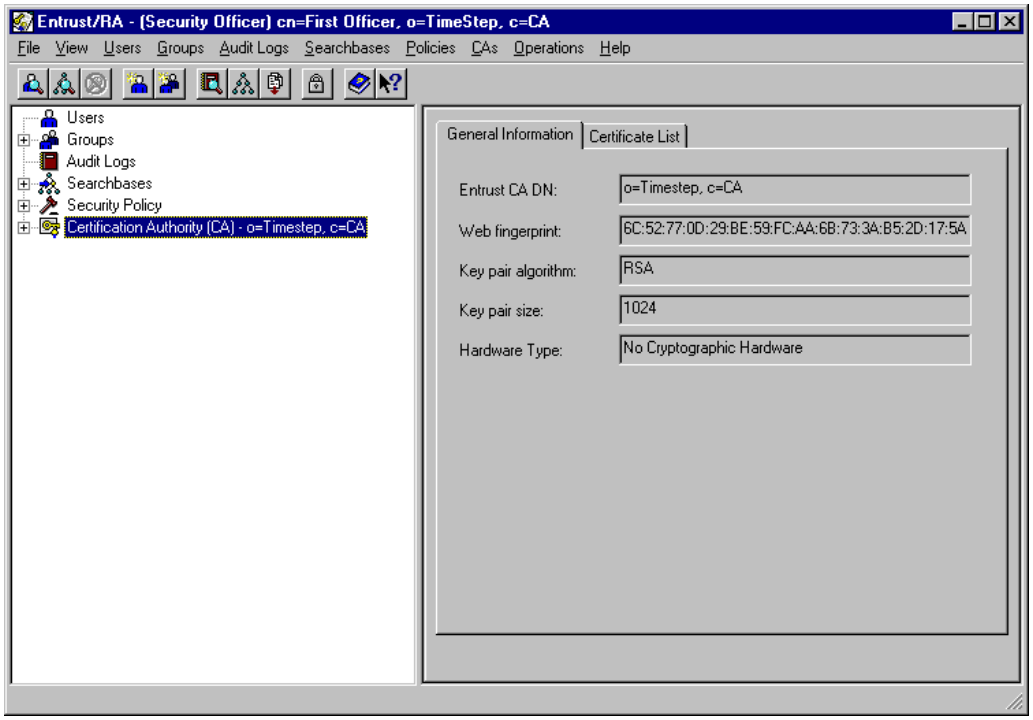
Creating a New User and perform offline profile

What I'm gonna do here is to create a profile for a new user and load it onto a Token Card for further distribution to employees, so they are not challenged for online certificate enrollment.

Make sure Entrust Service is up and running. To do so, open the control panel, click on Services and look for Entrust/Authority Service. Verify, that this service is running.

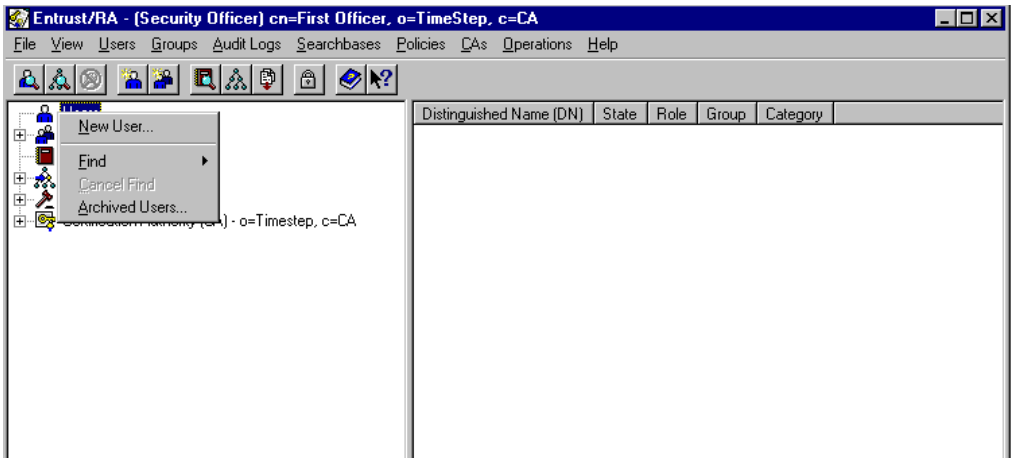
Logon to the Entrust RA and use "First Officer"

When logged on, you see the main window

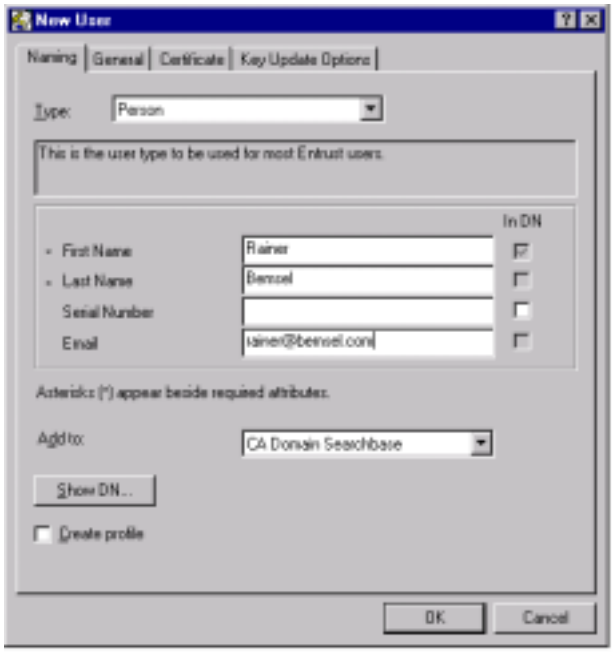


Add User

Right click Users in the left plane and select ***NEW USER***



The New User window pops up. (See next page)

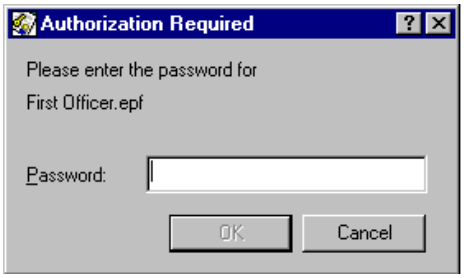


Type in following mandatory values

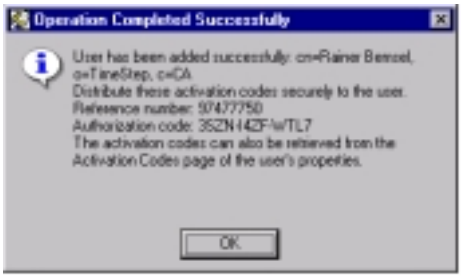
First Name **Rainer**
Last Name **Bemsel**

You could use any name, just make sure you remember, when configuring VPN Client

You will be asked to confirm the password to be allowed of creating this user



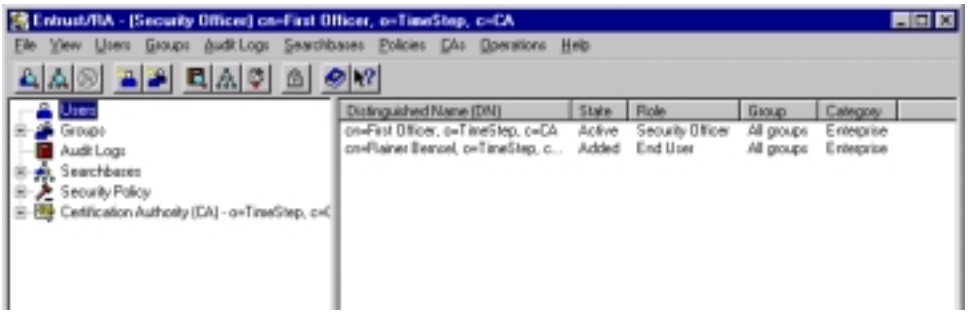
When done, you get Reference Number and Authorization Code back



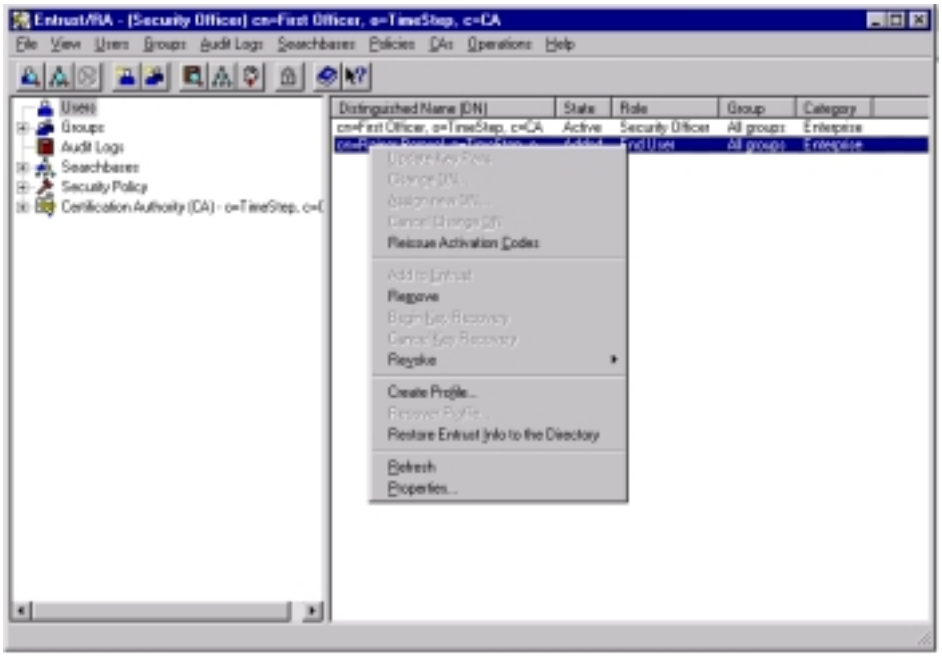
Select the ***Enable*** for Entrust Checkbox

Click OK to accept the ***Operation Completed Successfully*** info box

Back again in the main window, you will now see, that a new user did appear. Look at the State, which says ***Added***.



Highlight this new user and do a **right click**



Choose ***Create Profile***

Mark the checkbox on Store profile on hardware token

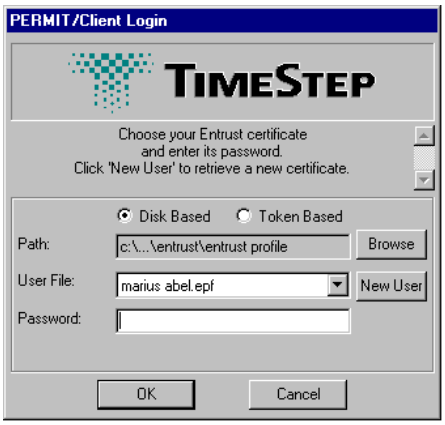
Set the Password to ***TimeStep1*** for the End User. If you choose a different password, make sure you have understood the Password Rules

Check your work

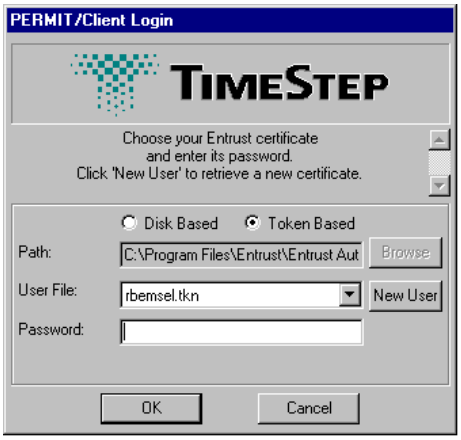
I have installed the PCI support for Token on my Entrust Certificate Authority and also have installed the PCMCIA support for Token on my VPN Client.

All I got to do right now is to verify if this works.

Start your client PC with TimeStep VPN Client installed, do a right click on the "**T**" and choose Login User

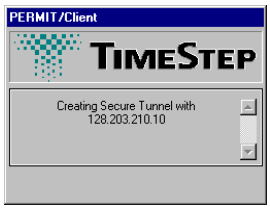


When used it before with Disk Based Certificates, you should see your last used Profile. Now change from Disk Based to ***Token Based*** and there you should see another profile with the extension of *.tkn. This has been downloaded via Entrust Certificate Authority.



Type in the proper password, which has been set during the profile creation earlier on, and click on **OK**

You will get a message to establish a secure link.



On the other hand, you may encounter a problem that the Peer is not responding. The first thing you have to verify, is your network link still OK (it used to work before, however, you have added a new PCMCIA card, which might influence the network card)

When this happens, following occurred: ⇨ I didn't read the readme file in ***c:\luna\ethcdfix***. ☹ or ☺

I have:

a) a notebook configuration running Windows NT 4.0
b) where one or more Luna tokens are being used in conjunction with other PC cards, (e.g. an Ethernet)
c) The other PC card is not functioning correctly

What happened?

The driver for the Luna tokens assumes that every PCMCIA slot (potentially) contains a Luna token. This behavior may cause other PC cards in the PCMCIA slots to malfunction.

Solution:
The driver for the Luna tokens needs to be explicitly told what slots contain Luna tokens. Therefore there are some batch files on ***c:\luna\ethcdfix*** to process the proper setting.

Done the batch and rebooted, I was able to establish a Security Association using the profile stored LUNA 2.