

For this Technical Tip, I've used a 3<sup>rd</sup> Party product, called LUNA 2. More detailed information on LUNA 2 could be retrieved via <u>www.chrysalis-its.com</u>. If you need a contact name within Chrysalis-ITS, please send an email to <u>rainer@bemsel.com</u> 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

Copyright 2001 Rainer Bemsel www.bemsel.com - rainer@bemsel.com

SwitchExpert CUBE



This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.

Page 1 of 15





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

CardWare Setup	×			
	Setup vill install CardWare in the following directory.			
	To install to this directory, click Next.			
	To install to a different directory, click Browse and select another directory.			
	You can choose not to install CardWare by clicking Cancel to exit Setup.			
<b>*</b>	Destination Directory			
	C/Program Files//DWNT Browse			
	< Back Newt> Cancel			

Accept the default directory and click on NEXT

Copyright 2001 Rainer Bemsel www.bemsel.com - rainer@bemsel.com











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

andware Setup	×
	Setup will create a new hardware profile for the CardWare drivers. Use this profile for working with TouchStare CardWare drivers. You can use other profiles to working with standard PCMEM drives.
:	Enter name of new hardware profile: [TouchStone CardWare profile
Ś	P Set new hardware profile as gelauit (recommended)
	<brck reg=""> Cancel</brck>

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

-	Please select outon Cart running Set.	t the Cardwi Mare installa Ip again	se op ilon a	tions to install." Ind add more of	You can create a ptions later by
•	두 Soci 두 Cad 두 Cad 두 Cad	et Services Services Ware compor la Casdwiare	verits Group	l I	Fler
<u> 1</u>	Target Dir S	pace		- System Dir S	pace
	Required	2388	KВ	Required	2398 KB
	Available	2005065	KВ	Available	2005065 KB

Copyright 2001 Rainer Bemsel <u>www.bemsel.com</u> - rainer@bemsel.com

Page 3 of 15







Deselect CardWare components and Create CardWare Group

Program	Boot	Sectors	êuto.	Marsual	Djoable	Command (ine
PCCS.SYS	9			Г	Г	/SCOFF /NC15
SSPCIC.SYS	R			Г	Г	AS AUTO IMPON APON
						d farmed for a d

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

Copyright 2001 Rainer Bemsel www.bemsel.com - rainer@bemsel.com





This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.

Page 4 of 15



Disk1 File Edit Vi	ew Help			_ O X
Name		Size	Туре	Modified
Disk1		OKB	File	7/14/00 9.39
Luna_CSC		SKR.	Setup Information	7/14/00 9.39
Luna_CS	Open		System file	7/14/00 9.39
README	Install		Text Document	7/25/00 4:44
	<u>Prink</u> <u>Q</u> uick View Add to <u>Zip</u>			
1	Segd To	•		1
	Cu≵ ⊈opy			16
	Create Shortos Delete Renage	4		
	Properties			

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

Copyright 2001 Rainer Bemsel www.bemsel.com - rainer@bemsel.com







Page 5 of 15



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

Welcome	×
	Welcome to the Luna Token Distribution for Entrust Entelligence Setup program. This program will install Luna Token Distribution for Entrust Entelligence on your computer.
	It is strongly recommended that you exit all Windows programs before running this Sietup program.
	Click Cancel to guit Setup and then close any programs you have running. Click Next to continue with the Setup program.
C.	WARNING: This program is protected by copyright law and international treates.
<b>*</b> >	Unauthorized reproduction or distribution of this program, or any portion of it, may seculi in severe civil and cimimal penalties, and will be prosecuted to the maximum extent possible under law.
	<pre>Sincel</pre>

Click on NEXT

Copyright 2001 Rainer Bemsel www.bemsel.com - rainer@bemsel.com

Page 6 of 15

Switch Expert



## Implementing Token Based Certificates with VPN Client



	Setup will install Luna Token Distil in the following directory.	bution for Entrust Entelligence		
	To install to this directory, click Next.			
	To install to a different directory, click Browse and select another directory.			
	You can choose not to install Lune Entelligence, by clicking Cancel to	a Takan Dishibution for Entrust exit Setup.		
<b>N</b>	Declination Directory			
	C.Yuna	Врания.		

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.

Copyright 2001 Rainer Bemsel www.bemsel.com - rainer@bemsel.com







Page 7 of 15





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.



Copyright 2001 Rainer Bemsel www.bemsel.com - rainer@bemsel.com

Page 8 of 15







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"

Copyright 2001 Rainer Bemsel www.bemsel.com - rainer@bemsel.com

SwitchExpert



This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.

Page 9 of 15





When logged on, you see the main window

🐼 Entrust/RA - (Security Officer) cn=First Officer, o	=TimeStep, c=CA
<u>File View U</u> sers <u>G</u> roups <u>A</u> udit Logs <u>S</u> earchbases <u>P</u>	tolicies <u>C</u> As <u>O</u> perations <u>H</u> elp
AA 🖉 🖀 🛤 🖪 A 🖗 🖄	
Users     Groups     Audit Logs     Searchbases     Security Policy     Certification Authority (CA) - o=Timestep, c=CA	General Information       Certificate List         Entrust CA DN:       o=Timestep, c=CA         Web fingerprint:       6C:52:77:0D:29:BE:59:FC:AA:6B:73:3A:B5:2D:17:5A         Key pair algorithm:       RSA         Key pair size:       1024         Hardware Type:       No Cryptographic Hardware

### Add User

Right click Users in the left plane and select NEW USER

Copyright 2001 Rainer Bemsel <u>www.bemsel.com</u> - rainer@bemsel.com







Page 10 of 15

# Implementing Token Based Certificates with VPN Client



🌠 Entrust/RA - (Security Officer) cn=First Officer, o=TimeStep, c=CA	
<u>File View U</u> sers <u>G</u> roups <u>A</u> udit Logs <u>S</u> earchbases <u>Policies</u> <u>C</u> As <u>O</u> perations <u>H</u> elp	
Distinguished Name (DN)       State       Role       Group       Category         Eind       Eancel Find       Archived Users       Image: Category (Image:	

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

New User Naming   General   Certifi	2 Key Update Options
Iype: Person	×
This is the user type to be	e used for most Entrust users.
- First Name - List Name	Rainer F Bernoel F
Serial Number Email	tainer@bennel.con
Astericks (*) appear besid	e requied attributes.
Add to:	CA Domain Searchbase
Show DN	
	DK Cancel

Type in following mandatory values

First Name Last Name Rainer Bemsel

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

Copyright 2001 Rainer Bemsel <u>www.bemsel.com</u> - rainer@bemsel.com







Page 11 of 15





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

🎆 Authoriza	ation Required	? ×
Please enter First Officer.e	the password for epf	
<u>P</u> assword:	I	
	OK Ca	ancel

When done, you get Reference Number and Authorization Code back

State of the second successfully	¢
User has been added successfully: cn-Rainer Bensel, on Tankfulp, cn/CA Dishibute frate activation codes securely to the user. Reference number: \$747750 Authorization code: 352NH425/WTL7 The activation codes can also be retrieved from the Activation Codes page of the user's properties.	
OK	

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*.

Entrust/IIA - (Security Officer) ca-First Of Ele Yew Uses Groups AuditLogs Searchio	licer, o-TimeStep, c-CA ases Policies DAs Operations <u>H</u>	eb.		
	No.	Sinte Bole	Guar	Calegory
R Group) Audit Logs R Searchbares R S Security Policy R Certification Authority (CA) - o+TimeStep, c=(	on-Fisi Ditioer, onTimeStep. c=CA con-Fisiner Illemont, onTimeStep. c	Adive Security Added End Une	Officer All groups	Erreprise Enteprise

Ν

Certified

NOVELL ENGINEER<sup>SM</sup>

Novell

Copyright 2001 Rainer Bemsel www.bemsel.com - rainer@bemsel.com

Switch Excer

Page 12 of 15



Highlight this new user and do a right click

Entrust/RA - (Security Officer) cn-First Officer File View Uners Brown: AuditLog: Searches	cer, e-TimeStep, c-CA sec Policies CA: Operations He	de d			- O ×
	N?				
Autorial     Autorial	Distriguished Name (DN) confirst Officer, on TreeStep, cn/CA District Officer, on TreeStep, cn/CA District Officer, on TreeStep, cn/CA Castory (DN) Castory (DN) Castory (DN) Castory (DN) Painter District Officer, office	State Active	Role Security Officer 7500 res	Group Al groups Al groups	Calegory Erdeprise Erdeprise
	Add to Jaytout Reginve Bagin bay, Hacovery Carrier Ser, Hacovery Registe	,			
	Create Profile Frommer Porte Restare Entrust (who to the Dir	ectory			
	Belenth Bioperties				

#### 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

Copyright 2001 Rainer Bemsel <u>www.bemsel.com</u> - rainer@bemsel.com





This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.

Page 13 of 15



Choose your Entrust certificate and enter its password. Click 'New User' to retrieve a new certificate. © Disk Based © Token Based Path: c:\\entrust\entrust profile Browse User File: marius abel.epf New User Password:	PERMIT/Cli	
Path:     C Token Based       Path:     Image: C Token Based       User File:     Image: C Token Based       Password:     Image: C Token Based	Click	Choose your Entrust certificate and enter its password. k 'New User' to retrieve a new certificate.
User File: marius abel epf  Password:	Path:	Disk Based     Token Based     Token Based     Browse
Password:	User File:	marius abel.epf
	Password:	

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.

PERMIT/Cli	ent Login
	ТімеЅтер
Clic	Choose your Entrust certificate And enter its password. k 'New User' to retrieve a new certificate.
	🔿 Disk Based 💿 Token Based
Path:	C:\Program Files\Entrust\Entrust Aut Browse
User File:	rbemsel.tkn 💌 New User
Password:	
	OK Cancel

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.

	TIMES	ΓEΡ
Creati	ing Secure Tunnel with 128.203.210.10	4

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)

www.bemsel.com - rainer@bemsel.com Copyright 2001 Rainer Bemsel







This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.

Page 14 of 15





When this happens, following occurred:  $\Rightarrow$  I didn't read the readme file in *c:Vuna\ethcdfix*.  $\bigotimes$  or  $\bigotimes$ 

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:Vuna\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.

Copyright 2001 Rainer Bemsel www.bemsel.com - rainer@bemsel.com

Switch Expert





This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.

Page 15 of 15