

Getting Started Guide

SmartCard 2.0

1.4



Table of Contents

Introduction.....	3
Who should read this document.....	3
PKI terms explained.....	3
Getting Started	5
Initial Requirements.....	5
1. Install VMWare player.....	5
2. Configuring the Server.....	5
3. Configuring the Client Workstation.....	8
4. Creating the Initial Administrator Card.....	9
5. Launching the ToLiMa Application.....	11
Other Configurations.....	12
Configure Apache Web Server to Test SSL Client Authentication.....	12
Windows SmartCard Logon.....	12
Appendix A, References and Links.....	13
Contacts.....	13
More Documentation.....	13

Introduction

This document will guide you through the steps involved in setting up the evaluation kit of ToLiMa called 'SmartCard 2.0' in your organization.

The evaluation kit contains four documents, the first is the one you are reading now, then there is a Card Administrators Guide explaining SmartCard management on a non-technical level, the next is a System Administrators Guide that describes further options in ToLiMa and more in-depth explanations of what is actually done and finally a guide that describes how to configure Microsoft SmartCard Logon.

Included in the kit are also two card readers, 5 SmartCards and one DVD containing all the software you need to set up a proof-of-concept of SmartCard management.

All you need before starting is one Windows XP or Vista workstation and the installation process shouldn't take more that a few hours.

Who should read this document

The intended audience are people involved in installing and configuring SmartCard 2.0 and want to evaluate what ToLiMa has to offer regarding SmartCard management. No previous experience of PKI or SmartCards is necessary.

PKI terms explained

Here are some of the common terms explained used during the SmartCard 2.0 configuration.

<i>Term</i>	<i>Explanation</i>
SmartCard 2.0	Compilation of all the components necessary to set-up a demo or proof-of-concepts of a SmartCard management system, customized for a specific organization.
ToLiMa	“Token Lifecycle Management”. The name of the actual SmartCard management application.
HTMF	“Hard Token Management Framework”. The framework that ToLiMa is built upon.
EJBCA	“Enterprise Java Bean Certificate Authority”, Open Source Certificate Authority that ToLiMa is integrated with.

CA	<p>“Certificate Authority”.</p> <p>A CA issues certificates to, and vouches for the authenticity of entities. The level of trust you can assign to a CA is individual, per CA, and depends on the CAs policy and practices statement.</p>
RA	<p>“Registration Authority”.</p> <p>An RA is an administrative function that registers entities in the PKI. The RA is trusted to identify and authenticate entities according to the CAs policy. There can be one or more RAs connected to each CA in the PKI. ToLiMa can be seen as a RA.</p>
Root CA	<p>A Root CA has a self-signed certificate and is also called Trusted Root. Verification of other certificates in the PKI ends with the Root CAs self-signed certificate. Since the Root CAs certificate is self-signed it must somehow be configured as a trusted root with all clients in the PKI.</p> <p>During the initial set-up of SmartCard 2.0 are four Root CAs generated. Used for Authentication, e-Signing, Microsoft Login and SSL Server certificates.</p>
Sub CA	<p>A subordinate CA, or Sub CA for short, is a CA whose certificate is signed by another CA, that can be another Sub CA or a Root CA. Since the Sub CAs certificate is signed by another CA, it does not have to be configured as a trusted root. It is part of a certificate chain that ends in the Root CA.</p>
End-entity	<p>An end-entity is a user, such as an e-mail client, a web server, a web browser or a VPN-gateway. End-entities are not allowed to issue certificates to other entities, they make up the leaf nodes in the PKI.</p>
AD	<p>Active Directory</p>
DN	<p>“Distinguished Name”, Name used in certificates to uniquely identity the user.</p>

Getting Started

Initial Requirements

Before you get started you need a workstation with Windows XP or Vista installed and administrative privileges. You will need two free USB ports for the SmartCard readers and at least 1 GB of RAM. The readers should install themselves automatically if it have access to Windows Update. If the workstation isn't connected to Internet you will have to install the driver for the SmartCard readers manually by running the installation by starting GemCCIDen-us_32.msi from the DVD.

1. Install VMWare player

In order to run the server software you need VMWare player installed. Because of licensing issues the software cannot be distributed on the DVD but must be downloaded manually through their website at : <http://www.vmware.com/products/player/>

Use all the default options during the installation.

If you already have VMWare workstation installed it may work as well but haven't been tested. If you want to run the image in VMWare server you may have to reconfigure the image before all the scripts run smoothly.

2. Configuring the Server

To start up the server you first need to unzip the image stored on the DVD to your hard drive. You can choose the actual location of the image yourself but that location will be referred to as '[c:\vmware-images](#)' throughout the rest of this document.

After the unzip operation is finished, just go to '[c:\vmware-images\smartcard20](#)' with a file explorer and double click on 'smartcard2.0.vmx' to launch the image. If you get a question if you have moved or copied the image, choose 'Copied it' and select 'Yes' on all other dialogs that might pop up.

The server will now boot. It is a Debian Linux installation with all the necessary software pre-configured.

When the server is up and running you see a login prompt:

```
Debian GNU/Linux 4.0 smartcard20 tty1
smartcard20 login:
```

Login with the username 'sc20' and the password 'sc20' to get to a command prompt. The first you have to do is to retrieve the IP address assigned to the server. This is

done with the command, 'ifconfig' and you will get the following output. The IP address is marked with bold text.

```
htmf@smartcard20:~$ /sbin/ifconfig
eth<n>   Link encap:Ethernet  HWaddr <nr>
        inet addr:x.x.x.x  Bcast:192.168.0.255  Mask:255.255.255.0
        inet6 addr: fe80::20c:29ff:fe60:2c68/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1492  Metric:1
        RX packets:390 errors:0 dropped:0 overruns:0 frame:0
        TX packets:132 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:35195 (34.3 KiB)  TX bytes:14209 (13.8 KiB)
        Interrupt:177 Base address:0x1400

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

This IP address have to be mapped, either in the workstations local host configuration file or in the DNS to the name 'smartcard20.demo'. To add it the the local host file you need to edit the file 'c:\windows\system32\drivers\etc\hosts' and add a row containing:

```
<IP-Address> smartcard20.demo
```

To exit the VMWare player console press the keys 'Ctrl+Alt'.

Then enter the VMWare player console again by clicking in it's window and issue the command (exactly as it is written):

```
htmf@smartcard20:~$cd /usr/local ; sudo ./htmf-setup
```

First you will be asked for a password, enter 'htmf' again.

This will start the installation process and will result in a configured demo PKI and a client installation package customized for your organization. This step will take a couple of minutes to complete.

You will see the following output on the screen:

```

Welcome to ./htmf-setup, a tool to install htmf for PoC/Demo Purpose
Will  and copy in a new version
This will make all you issued cards no usable in the new installation, ie
you will need to blank them first
Enter to continue, ctrl-c to abort

To follow the verbose output of the install in a new screen run: tail -f
/tmp/smartcard20-setup.2645
Step 1/9 Cleaning out old jboss-files (and installing a fresh copy): ok
Copying in new jboss-files: ok
.....
<Then is all nine steps required for configuring the EJBCA and ToLiMa
installation package done one by one>

.....
Step 9/9 Restarting Jboss: Stopping JBoss: (not running).
Starting JBoss using Java from /usr/local/java: /usr/local/htmf
jboss4.
done
Open http://smartcard20.demo/ for continued installation instructions
    
```

The script will ask the following questions during the installation:

<i>The name of your organization</i>	Use only regular letters, numbers and spaces in the name.
<i>The hostname of the CA server</i>	The hostname used to refer to this server in the entire configuration, here you can use smartcard20.demo or a name you define yourself but it must be registered in the DNS or in the host file of all the computers used in the evaluation.
<i>Enter the domain name of your Active Directory</i>	The domain part of the UPN, for instance if your users have a UPN of user1@ad.someorg.org you should enter 'ad.someorg.org'
<i>Enter the hostname to the SMTP server</i>	The hostname or IP address to the SMTP server in the organization, since only internal e-mails will be sent there probably won't be any need for SMTP Auth settings. If it is still required, you edit it in the file global.properties and is explained in the section 'Reconfiguring ToLiMa Manually ' in the System Administrators Guide.
<i>Enter the email address of the administrator that should approve requests by non-admins</i>	Best way is to use an alias, but someone's regular e-mail address will probably be sufficient during the evaluation.
<i>Enter the email address used in the from field of approval mails</i>	Used in the from field and should be an address that can be relayed in the SMTP server.
<i>Enter the text displayed when a non-admin is waiting for approval.</i>	Text used to describe for regular users how to come in contact with the approval administrator, can be a e-mail address or telephone number. The text can be displayed on three rows but each row shouldn't contain more than 50 characters.

When the script has finished you are done configuring the server. If you later want to reconfigure your settings, just rerun the 'htmf-setup' command and you will remake the installation from scratch.

If you want more verbose output of what is actually happening during the installation process you can look in the file /tmp/smartcard20-setup.<number> in the server.

3. Configuring the Client Workstation

The preparation of the workstation used for Card Administration is done in three simple steps.

- First, install the Java JRE shipped with the distribution at <http://smartcard20.demo/jre-6u11-windows-i586-p.exe> . Be sure you use that version of the JRE even if you already have another one installed.
- Install the NetID client that PKI software use to communicate with the SmartCards. Download it from <http://smartcard20.demo/iidsetup.exe>

If you want another card administration station just repeat the steps above.

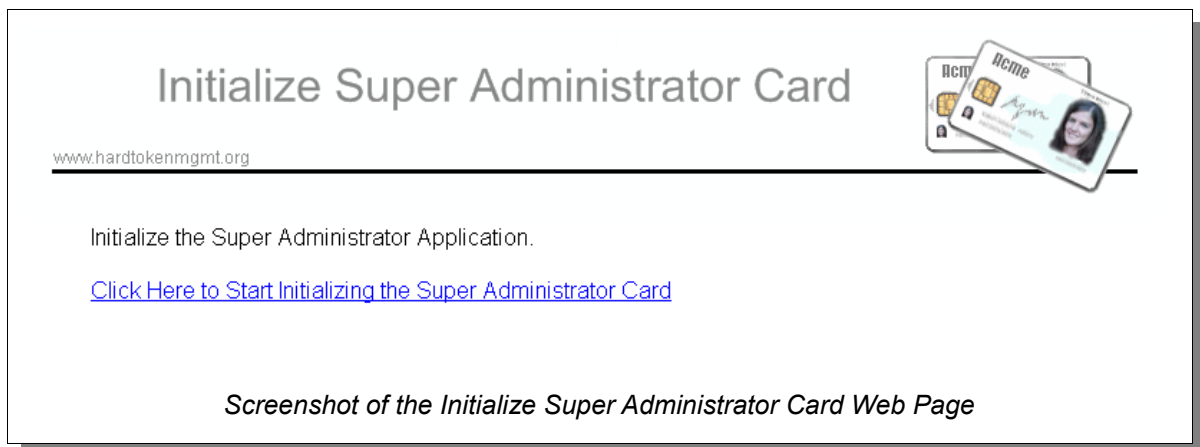
If you need a computer that just use the SmartCards you only need to install the NetID software and optionally the card reader drivers if they aren't installed automatically.

4. Creating the Initial Administrator Card

You need an initial administration card used to authenticate the administrator to the ToLiMa application. In the evaluation kit you have one card marked 'Super Administrator'. Insert that into one of the card readers and start up a browser and go to the URL:

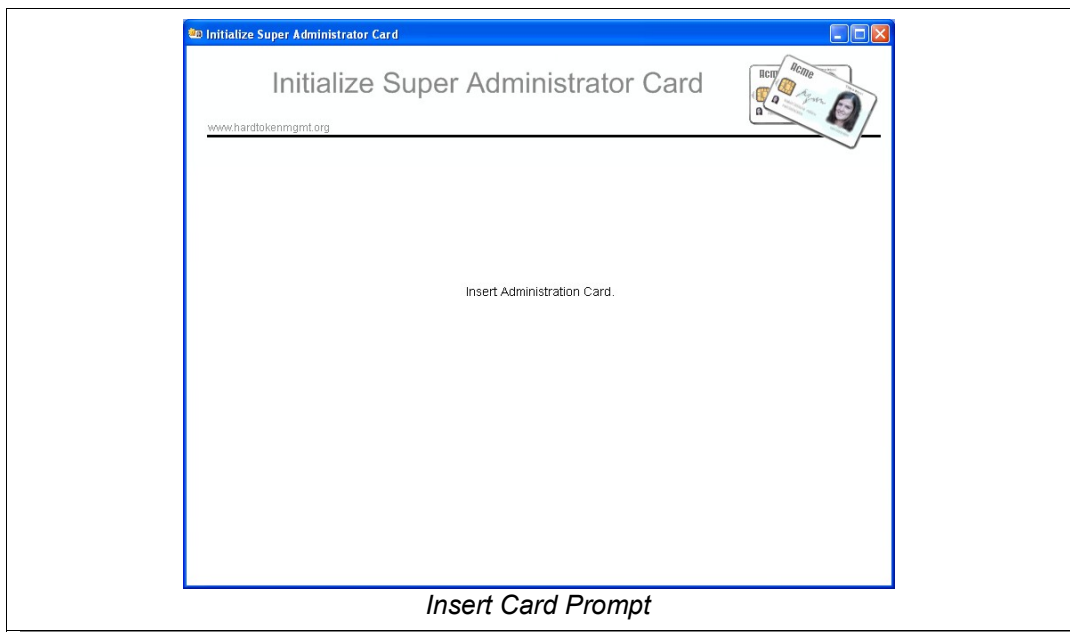
<https://smartcard20.demo:8442/htmf/isa.jsp>

You will get to the following page, Click on 'Click Here to Start Initializing the Super Administrator Card' to start the application..

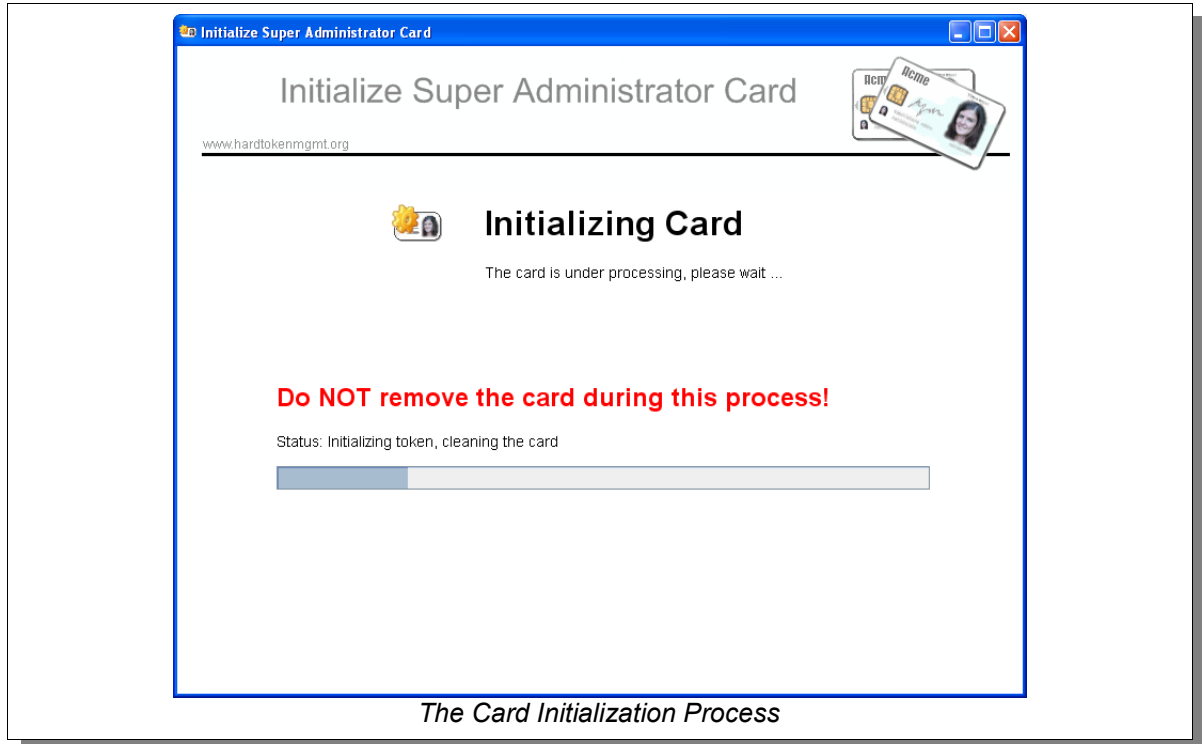


The program is delivered with Java Web Start so you may need to click some check boxes to approve the issuers of the program packages.

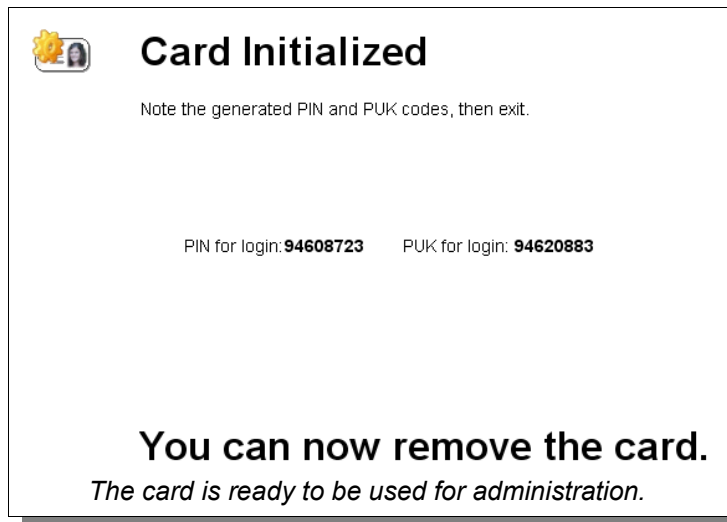
When the application have started the following prompt will appear (unless the card is already inserted, when will the initialization start directly).



Insert the card and the process will begin automatically. The following page will be shown:

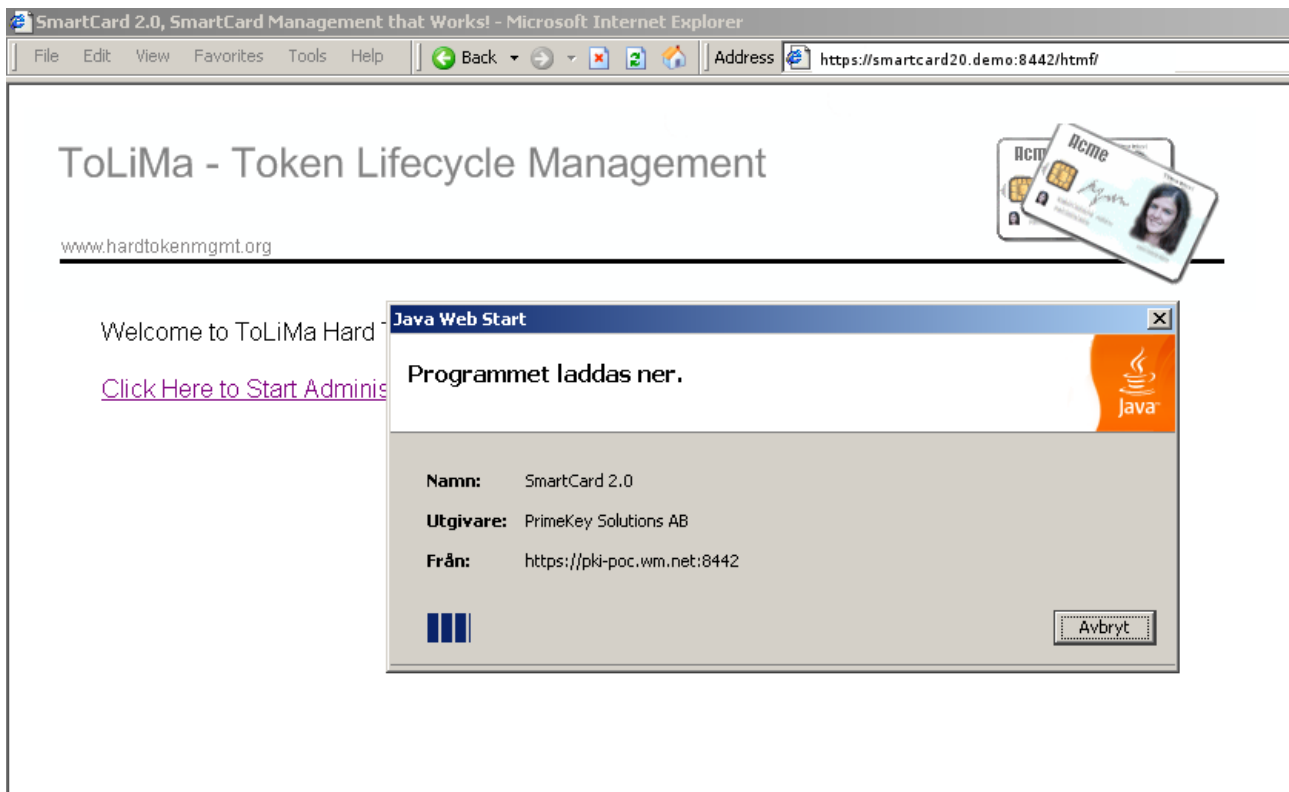


When the process have finished will the PIN and PUK codes of the generated card be shown, they are randomly generated and it is a good idea to write these down. It is possible to copy and paste the codes. When the codes are saved you can close this application.



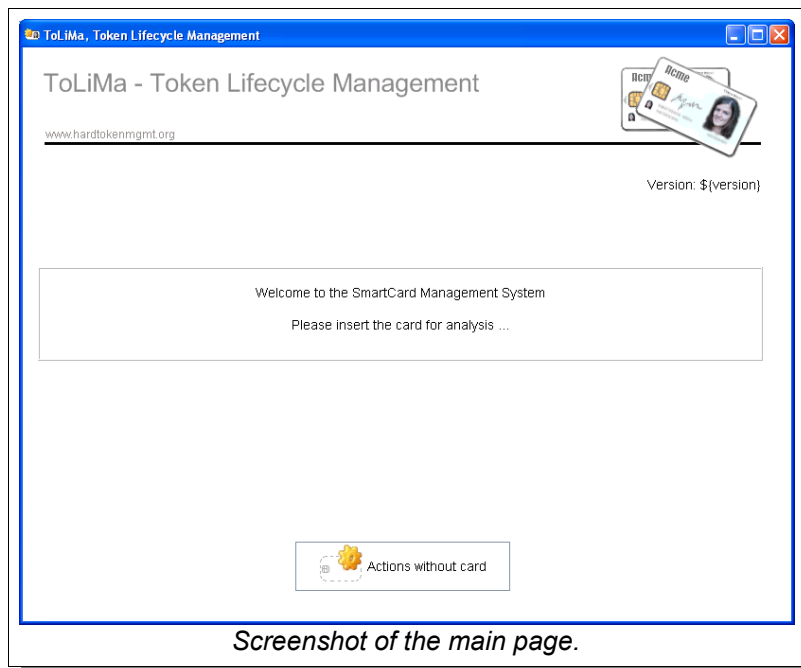
5. Launching the ToLiMa Application

The final step is to launch the ToLiMa Application. The program is delivered with Java Web Start so you may need to click some check boxes to approve the issuers of the program packages. Open your browser and go to the URL: <https://smartcard20.demo:8442/html/>



First you will be prompted to Insert the administration card if it isn't inserted already. Then enter the PIN of the card and click on 'Logon' to authenticate yourself to the server.

If the log-in was successful you are all set to start administrating SmartCards. You can read more about SmartCard administration in the document 'Card Administrators Guide'.



Screenshot of the main page.

Other Configurations

Configure Apache Web Server to Test SSL Client Authentication.

One of most used applications of SmartCards is secure logon to web pages. In this evaluation kit there is a script configuring an apache server used to test SSL client authentication. To run the script, goto to the VMWare player console and issue the commands:

```
# cd /usr/local  
# sudo htmf/src/inst/smartcard20/configure-apache.sh
```

Then test to logon to the web server using any of the issued SmartCards by going to the link <https://smartcard20.demo/test-your-certificate.cgi> and you will see a simple page here you can find the name of the SmartCard owner.

Windows SmartCard Logon

How to configure your Active Directory for SmartCard Logon is described in a separate document that is included in the evaluation kit.

Appendix A, References and Links

Contacts

Integrator and developer of the ToLiMa / HTMF projects

<http://www.logica.se>

Developers of EJBCA:

<http://www.primekey.se>

Developers of NetID client:

<http://www.secmaker.se>

Card and Reader Manufacturer

<http://gemalto.com/enterprise/product/index.html>

More Documentation

Smartcard 2.0:

<http://www.smartcard20.com>

ToLiMa project Main Web Site:

<http://www.hardtkenmgmt.org>

ToLiMa Flash Demo:

http://www.hardtkenmgmt.org/viewlet/ToLiMa_viewlet_swf.html

EJBCA Main Web Site:

<http://www.ejbca.org>