

System Administrators Guide

SmartCard 2.0



1.3

Administration Guide

MS SmartCard Logon Guide

PDF Signing Guide

Table of Contents

| | |
|--|----|
| Introduction..... | 4 |
| Who should read this document..... | 4 |
| PKI terms explained..... | 4 |
| Administration Guide..... | 7 |
| Introduction..... | 8 |
| Administrating ToLiMa..... | 8 |
| About ToLiMa..... | 8 |
| The ToLiMa Installation Package..... | 8 |
| Reconfiguring ToLiMa manually..... | 8 |
| Editing the global properties..... | 8 |
| Changing the resource files..... | 9 |
| Importing existing User Data..... | 9 |
| Integration with Authorization Systems..... | 9 |
| Managing Errors..... | 9 |
| Log Files..... | 9 |
| Administrator settings..... | 10 |
| Generating Technical Error Reports..... | 10 |
| Basic EJBCA Administration..... | 11 |
| Different Administrator Roles..... | 11 |
| Card Administrator..... | 11 |
| System Administrator Card Administrator..... | 11 |
| Super Administrator..... | 11 |
| Approval Administrator..... | 11 |
| Adding an Administrator..... | 11 |
| Adding Administrative Privileges..... | 12 |
| Setting the Administrator flag..... | 13 |
| Approving a non-Administrator Request..... | 14 |
| Using the E-mail Link | 14 |
| Manually Finding a Request to Approve..... | 15 |
| Functional Explanation of ToLiMa..... | 16 |
| The Main Page..... | 16 |
| Generating Tokens..... | 17 |
| Renew Token..... | 18 |
| Unblock Token..... | 19 |
| Viewing Tokens..... | 20 |
| Revoke and Clean Tokens..... | 20 |
| Reactivate Tokens..... | 21 |
| Administrator Actions without the Card..... | 21 |
| Non-administrator Actions..... | 22 |
| MS SmartCard Logon Guide..... | 25 |
| Introduction..... | 26 |
| Enabling SmartCard Logon | 26 |
| Prerequisites..... | 26 |
| Request a Domain Controller Certificate..... | 26 |

| | |
|---|----|
| Install the Domain Controller Certificate..... | 28 |
| Install the MS CA Certificate..... | 28 |
| Propagate the MS CA Certificate to all Clients..... | 29 |
| Install CSP on Client Machine..... | 29 |
| Verify Setup..... | 29 |
| Logon with SmartCard..... | 32 |
| PDF Signing Guide..... | 33 |
| Introduction..... | 34 |
| Client signatures..... | 34 |
| Server signatures..... | 34 |
| Enabling PDF Signing..... | 34 |
| Prerequisites..... | 34 |
| Install the CA certificate in Adobe Acrobat..... | 35 |
| Signing documents..... | 35 |
| Verifying signed documents..... | 37 |
| Appendix A, References and Links..... | 39 |
| Contacts..... | 39 |
| More Documentation..... | 39 |

Introduction

This document describes some of the options and possibilities of ToLiMa from a System Administrators point of view. The guide is divided into three major sections:

- Administration guide – describes administration of ToLiMa and EJBCA.
- MS Smartcard Logon guide – describes how to setup smartcard logon on windows systems using ToLiMa and EJBCA.
- PDF Signing guide – describes how to sign PDF documents usgin smartcards and Adobe Acrobat.

Who should read this document

The intended audience are system administrators that want more in-depth explanations about ToLiMa and wants to set up real applications to use smart cards.

PKI terms explained

Here are some of the common terms used with ToLiMa, both application specific and general PKI related that can be good to know before starting the deployment.

| <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 | “Certificate Authority”. 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. |
| RA | “Registration Authority”. 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. |
| 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 CA's self-signed certificate. Since the Root CA's 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 CA's 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> |
| CRL | <p>"Certificate Revocation List". A file containing all the serial numbers of the certificates that have been revoked and shouldn't be trusted any more. A CRL is usually issued with a regular interval and is signed by the same CA that have issued the certificates.</p> |
| OCSP | <p>"On-line Certificate Status Protocol", Protocol for instant lookup of revocation status of certificates over the network.</p> |
| JBOSS | <p>World-wide used, open source based, J2EE application server used by EJBCA.</p> |
| AD | <p>Active Directory</p> |
| DC | <p>Domain Controller. The AD is accessed through Domain Controllers.</p> |
| DN | <p>"Distinguished Name", Name used in certificates to uniquely identify the user.</p> |
| PDF | <p>The <i>Portable Document Format</i> is the file format created by Adobe Systems for document exchange.</p> |

Administration Guide



Introduction

This part is divided into three sub sections, the first one describes how the default configuration works and the possibilities to enhance it. The second contains some basic information about EJBCA administration and the final section gives some more in-depth explanations of what actually happens in the different steps of the ToLiMa application.

Administering ToLiMa

About ToLiMa

ToLiMa stands for Token Lifecycle Management and is the first SmartCard management application built upon the Hard Token Management Framework. It have been developed with customers having a long experience of smart card usage and is adapted to their requirements to get a functional system that works in their organization.

It is an open source application that can be found at <http://www.hardtkenmgnt.org>.

The ToLiMa Installation Package

During the installation process of SmartCard 2.0 is a customized installation package of ToLiMa generated specific for the organization.

It is possible to distribute the installation package silently through a group policy i AD or similar using the '/S' option.

Reconfiguring ToLiMa manually

The default configuration of ToLiMa in SmartCard 2.0 is stripped down with no integration points to existing systems for a simplified set-up. It is possible to reconfigure the behavior of ToLiMa and regenerate the installation package manually.

This is done in the VMWare image using the commands:

```
#. /usr/local/environment
#cd /usr/local/htmf
#ant deploy
```

The generated application will automatically be deployed to the application server.

Editing the global.properties

The main configuration file is in the 'src/resources/globalsettings/global.properties' and controls the actual behavior of ToLiMa. More details about configuring can be found in the actual file and in the developers handbook found at the URL:

<http://www.hardtkenmgmt.org/developersguide.html>.

Another configuration file controlling the actual build process of ToLiMa, such as the name used in the in the start menu is configured in the file 'hardtkenmgmt.properties' i the base 'htmf' directory.

Changing the resource files

It is also possible to change language resources and images. This is done in the directories. 'src/resources/languages' and 'src/resources/images'. Remember to regenerate the installation package after editing these files.

It is also possible to have custom developed code and resources separated from the open source project code for easier maintenance. This is explained further in the developers guide.

Importing existing User Data

If it is desired to have ToLiMa to look up the name automatically using the unique user id there is a need for a customized plug-in called UserDataSource that is loaded into EJBCA.

This can be very useful since it reduces the amount of work for the card administrator when issuing the card and eliminates the risk that the administrator enters the wrong name when issuing a batch of users from a list.

It's also possible to have user data removed or edited from ToLiMa if a user returns his card when he leaves the organization. This is also done through the UserDataSource.

See <http://www.ejbca.org/manual.html#Framework%20for%20External%20User%20Data%20Sources> for more information about writing a customized UserDataSource.

Integration with Authorization Systems

It is also possible to integrate ToLiMa with existing authorization systems. This is done by creating a plug-in called 'Publisher' that is used to signal to other systems when a certificate is issued or revoked.

See <http://www.ejbca.org/manual.html#Custom%20publishers> for more information about how to develop such a plug-in.

Managing Errors

Log Files

There are two log files that can be reviewed if something goes wrong. One is on the server and one on the local workstation.

The server log file written by the EJBCA application is placed in
/usr/local/jboss/server/default/log/server.log

ToLiMa logging is written to the file .hardtokenmgmt_<nr> in the card administrators home directory.

Administrator settings

Disabled in the SmartCard 2.0 configuration is the possibility to let the administrator configure their preferences. It is possible to configure so the administrator settings tab is displayed the first time the administrator start up the application.

These settings are configured in a property file in the administrators home directory. Usually two files are created. One is `adminsettings_default.properties` which contains information stored before the actual administrator have logged in. The other one is the settings file stored in `adminsettings_<certificate SN>.properties`.

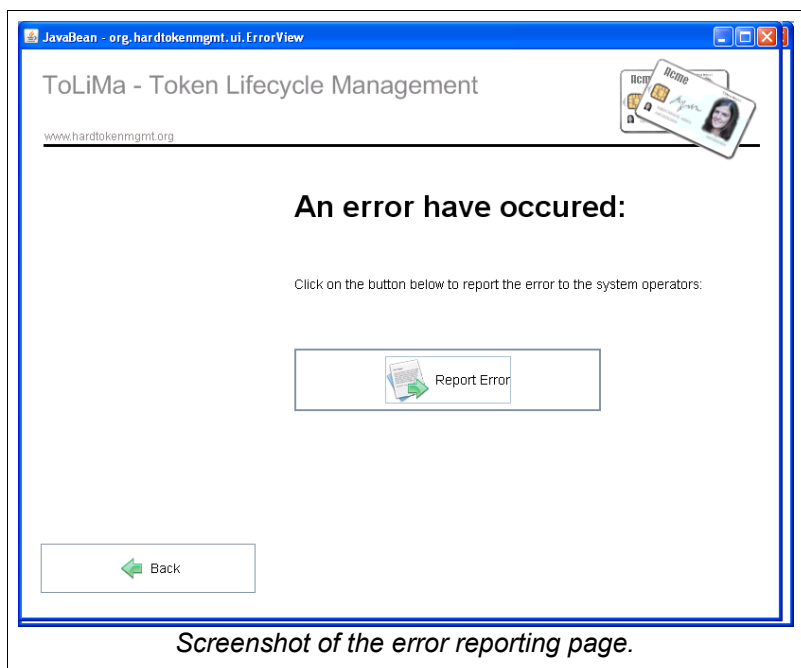
Remove the files to reset the settings.

Generating Technical Error Reports

With ToLiMa it is possible to have technical error reports sent to the technical administrators instead of displaying a confusing error message to the card administrator.

It can be configured with the following functionality:

- Always send reports to a dedicated email address. Useful for system administrators that want to know what errors actually occurs in their organization.
- Let the administrator choose if a report should be sent.
- Disable reporting and just display the name of the error for the card administrator. This is used in the default configuration for simplified set-up of the demo.



Basic EJBCA Administration

The section describes some of the most important areas of EJBCA administration during the demo of SmartCard 2.0 such as adding administrators or approving requests.

If you are more interested in learning the details of how to configure and administrate EJBCA there are tutorials at <http://wiki.ejbca.org/admintutorials>, and more general information at <http://www.ejbca.org>.

Different Administrator Roles

Using SmartCard 2.0 there are three preconfigured administrator groups covering the three basic roles involved in managing SmartCards. The roles are: Card Administrator, Super Administrator and Approval Administrator. Each one is explained below.

Card Administrator

Card administrator is a user with privileges to issue cards, unlock PINs, revoke cards and so forth without requiring an approval from a second party.

System Administrator Card Administrator

The same as Card administrator but also have the possibility to issue System Administrator cards, i.e. cards that system administrators can log-in to systems with administrative privileges. By default is this done by adding 'adm' to the username in the windows UPN. For example if a user have an ordinary card with UPN of phive@someorg.org the card issued with administration profile will have an UPN of phiveadm@someorg.org. This should not be confused with Card Administrator cards.

Super Administrator

The main administrators of EJBCA that have overall superuser rights (like root access in Unix). The initial administration card issued in the installation process of SmartCard 2.0 belongs to the Super Administrator group.

Approval Administrator

Approval administrators have the right to approve request by regular users to unblock PIN and issue smart cards. Usually is this role assigned to a central help-desk or support unit to verify the identity of the users during non-business hours or when a card administrator isn't physically available.

Adding an Administrator

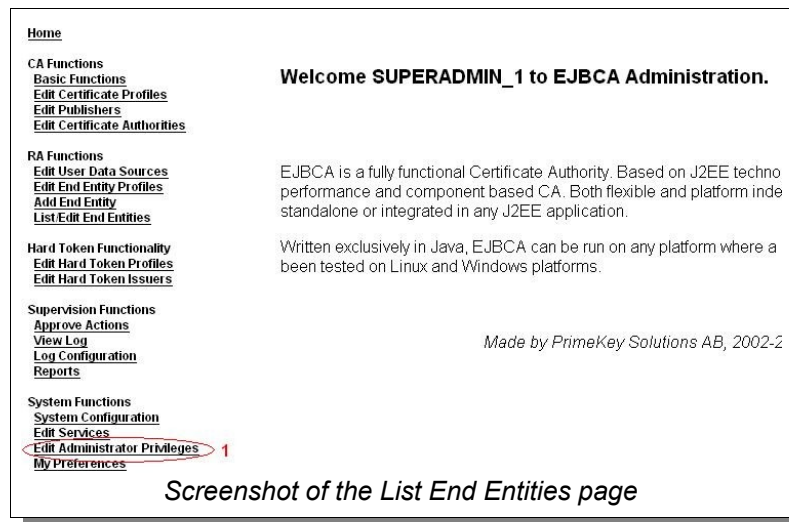
Adding an administrator is done in three steps:

- First issue a card to the user using ToLiMa
- Then add administrative privileges to that user.
- Finally mark the user (called 'end entity' in PKI terms) with the administrator flag. This is flag is used as a backup to make sure no user get administrative privileges to the CA system by mistake.

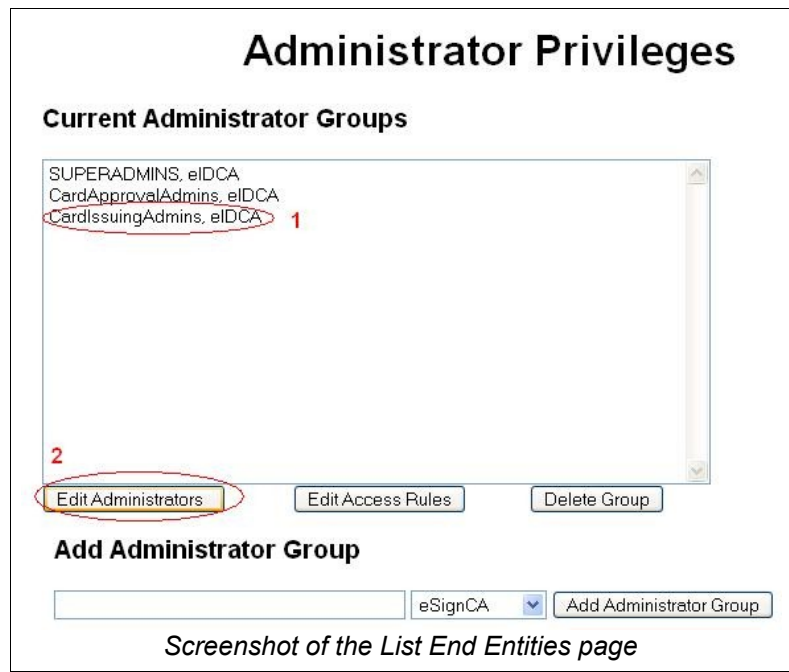
Steps 2 and 3 are configured in EJBCA . To log in to the administrative web interface, use the card issued in the initial installation and go to the URL <https://<hostname of SC2.0 installation>:8443/ejbca/adminweb>

Adding Administrative Privileges

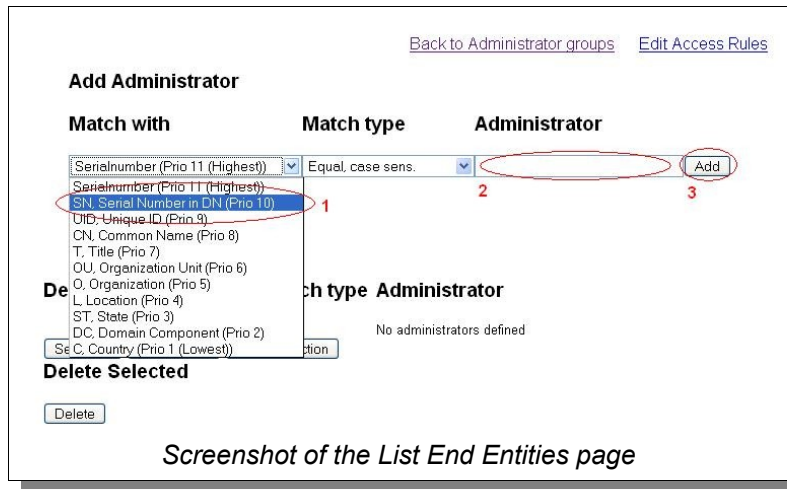
After logging in to EJBCA you will see the welcome page. To add privileges to a user click on 'Edit Administrator Privileges' in the bottom of the menu.



Then select the administrator group you want to add the user to and click on 'Edit Administrators'.

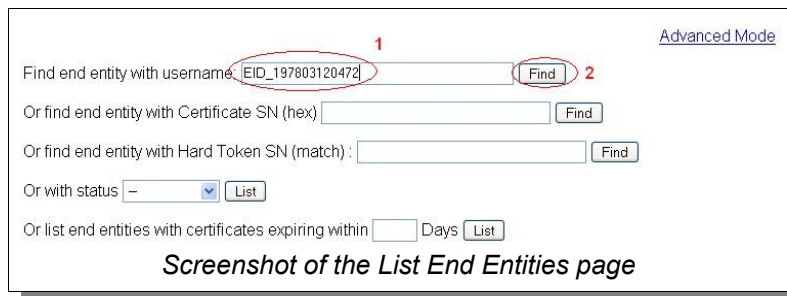


Finally select 'SN, Serial Number in DN (Prio 10)', enter the serial number of the user used when issuing the card and click on 'Add' and you are done with step 2.



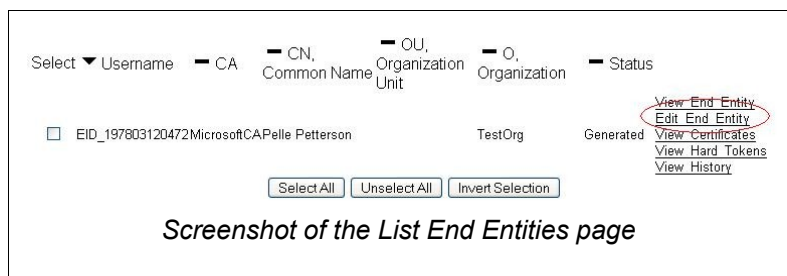
Setting the Administrator flag.

The final step is to mark the user as administrator, used as a safety against misconfiguration. First click on 'List / Edit End Entities' in the left side menu.



Then find the user to mark by entering the username of the end entity. The username is 'EID_<serial number of user>' and click on 'Find'.

If the user initially was issued successfully in ToLiMa it will show up in the listing below. Click in the link 'Edit End Entity' to view the details.



In the pop-up window, scroll to the bottom and check the check box 'Administrator' and click on 'Save'.



The user should now be able to log in and be a card administrator in the ToLiMa application.

Approving a non-Administrator Request

It is possible for regular users to perform PIN unlock and issue spare cards through a colleague but those actions have to be approved by a approval administrator.

Using the E-mail Link

As soon as a request is generated an email is sent to the approving administrators containing a link to a approval request review page. This page contains enough information for the approving administrator to approve or reject the request.

As soon the request is approved it is possible for the colleague to continue with the PIN unlock or spare card generation. The ToLiMa application can be closed during the waiting but an approval is only valid for eight hours (in the default configuration) before a new approval request have to be generated.

Generate Token

Current Status : Waiting

| | |
|----------------------------|--------------------------|
| Request Date | 2008-apr-01 15:44:22 |
| Expire Date | 2008-apr-01 23:44:22 |
| Requesting Administrator | Pelle Petterson, TestOrg |
| Related CA | eSignCA |
| Related End Entity Profile | EEP_eID |
| Remaining Approvals | 1 |

Requested Action Data

Subject DN : CN=sadf asfd, SN=123456789012,O=TestOrg
 Label : Temporary Card
 Username: [EID_123456789012](#)

Approved By

| Action | Date | Administrator | Comment |
|-------------|------|---------------|---------|
| None | | | |

Screenshot of the Approval Request Review page

Manually Finding a Request to Approve

It is also possible to manually find an approval request by logging in to EJBCA at the URL <https://<hostname of SC2.0 installation>:8443/ejbca/adminweb> and click on 'Approve Actions' in the menu to get a listing of waiting requests.

By clicking on the desired request the same page as is referred to in the e-mail will be displayed.

Approve Actions

Search for action with status: requested within:

| Request Date | Approve Action Name | Requesting Administrator | Status |
|------------------------------|-------------------------------------|--|------------------------|
| 2008-apr-01 15:44:22 | Generate Token | Pelle Petterson, TestOrg | Waiting |

1 Approval requests found.

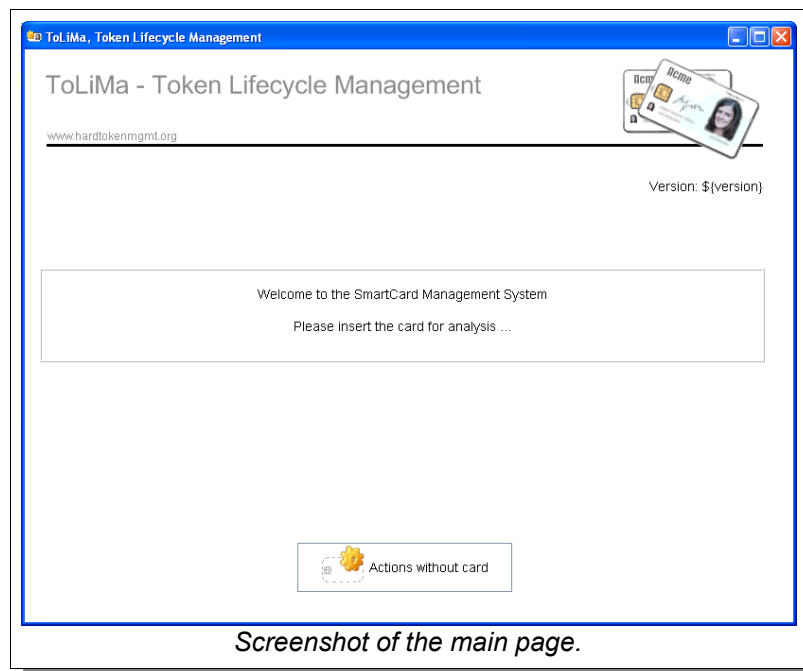
Screenshot of the List Approval Requests page.

Functional Explanation of ToLiMa

This section will give the details of what steps actually are performed under the hood during the different actions in the application and what can be configured in addition to the default SmartCard 2.0 configuration.

The Main Page

The main page is displayed directly after log-on by a card administrator, (if a processable card haven't been inserted already), performs the actual analysis of what could be wrong with the card and redirects the administrator to the appropriate page.



Some of the steps performed during analyses are:

- If the card is empty is the administrator redirected to generate new card page.
- A card that is about to expire (default is less that 10 days) will lead to the “renew card page”.
- If the card is blocked leads to the PIN unblock page.
- If the card is revoked to the generate card page.
- If the card is temporary revoked leads to the reactivate page.
- If the card seems normal is a simplified menu displayed with the options to view the details, revoke and clean or to re-activate the card.

There also exists a button that takes the administrator to the “Actions without card” menu.

Generating Tokens

The most advanced page of ToLiMa is for token generation. It's a a four step wizard where the steps are :

1. A unique user id is entered, and if ToLiMa is integrated with some form of existing user database is the rest of user's data fetched before the next step. Fetching external user data isn't supported in the default SmartCard 2.0 configuration.
2. In the next page is the name of the user entered in the default configuration.

If a UserDataSource is used instead will just the name be displayed with the option to override the information if it isn't correct. An overridden name will result in special logging in the EJBCA database for tracing purposes.

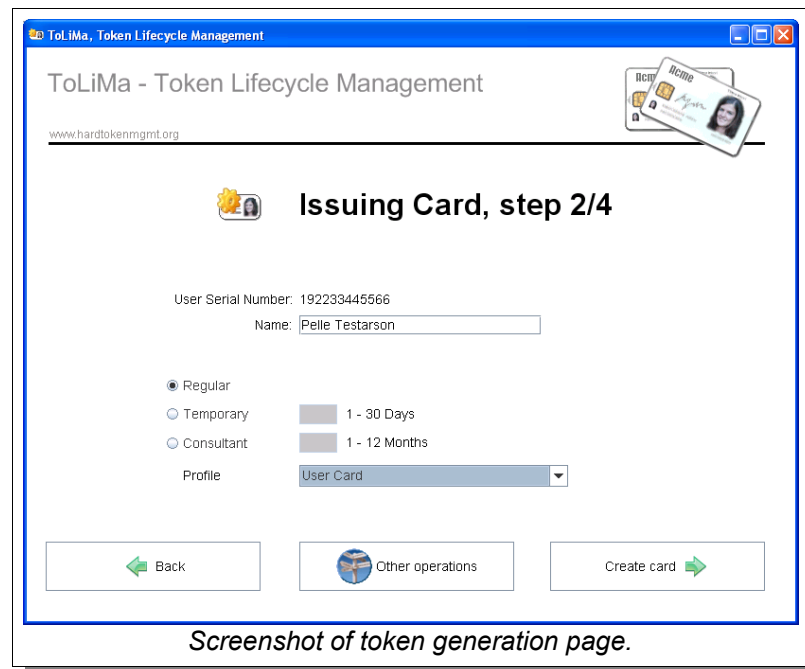
It is also possible to select the type of card to issue, the options are:

- Regular card, with 5 years validity
- Temporary card, or spare card with 1 to 30 days validity
- Consultant card valid for 1 to 12 months.

There also exists an option called 'Profile' that can have two options depending on your role as a card administrator. The available profiles are:

- User Card, i.e. a card a users uses for normal login.
- Administrator Card, a card containing the users credentials to log-in as system administrators. These are usually only issued to technical staff that needs a separate card with higher privileges in their systems. This is not to be confused with a Card Administrator, issuing a card with profile 'Administrator Card' does not mean that it can be used to log-in to ToLiMa.

Usually will only a special group of card administrators have access to the 'Administrator Card' profile.



3. In the third page is the actual token generation performed. There basically exists two types of cards, those that can be reinitialized and those that are pre-formatted in factory and cannot be initialized again. First is the card reformatted (if possible, otherwise is the keys regenerated and the two PINs reset. Then are three certificate requests generated that are certified by EJBCA before they are placed back on the card. The users old certificates are revoked, permanently for regular and consultant cards and temporarily (called 'on hold') for spare cards. It is configurable if spare card issuing should result in temporary revocation or not.

Important: If the card type cannot be reinitialized must the PUK codes be uploaded to the EJBCA database before the token can be personalized. Therefore are reinitializable cards strongly recommended.

4. In the fourth and final step is the user prompted to set his PINs. This can be reconfigured to either have a fixed or random PIN that is displayed or that the user is only prompted to enter one code which is set to both identification and signature PIN.

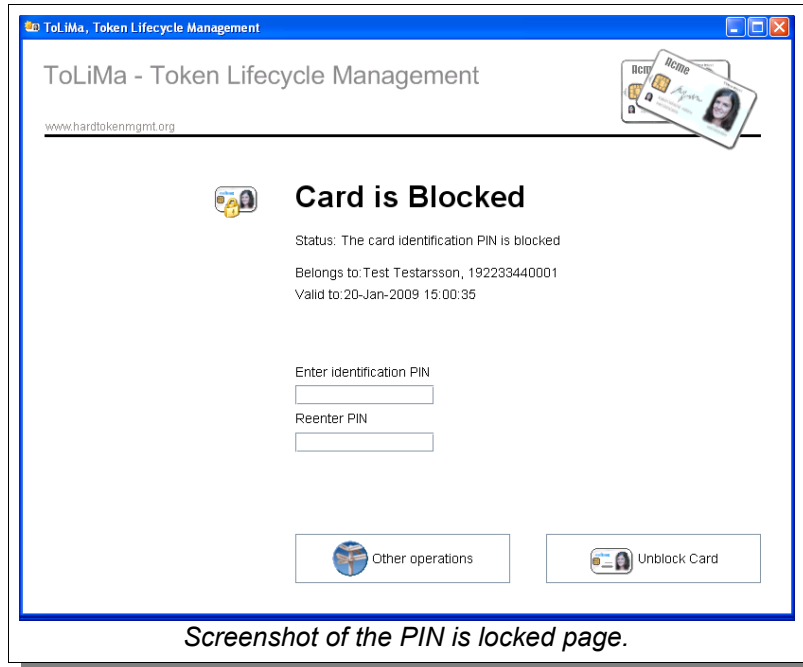
Renew Token

The renew token page that is the administrator either is redirected to if the card is about to expire or can be accessed manually through the view token page.

It quite simply removes the certificates on the card, generates new requests with the same validity as the original certificates and places them back to the card.

Unblock Token

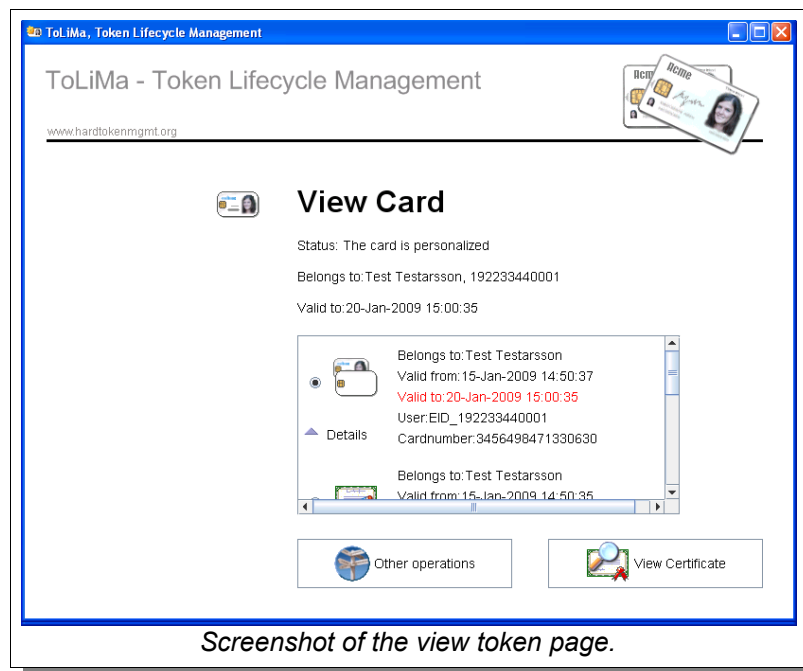
If the analyzer notices that one of the PINs is locked results in the unblock PIN page being displayed. The page fetches the PUK (that is stored encrypted in the EJBCA database), unlocks the PIN and lets the user set a new one.



Viewing Tokens

The view token page lets the administrator examine the certificates placed on the card. The card have a different logotype depending if it's issued as an ordinary, temporary or to a consultant. The certificates on the actual card also have different logotypes depending on usage.

From this page it is possible to view the information in a certificate separately.



Revoke and Clean Tokens

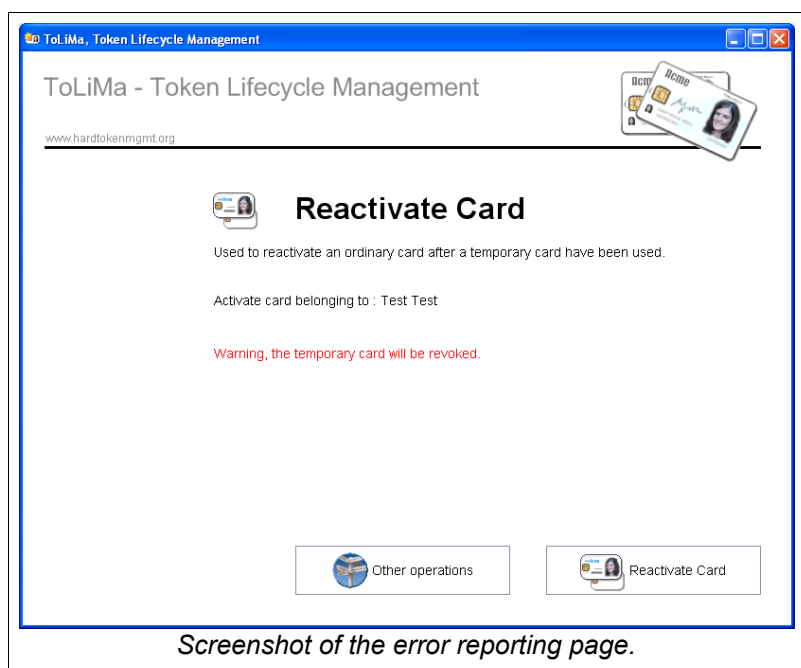
The revoke and clean page revokes the certificates on the card permanently and cleans the card (removes the keys and certificates) so it can be reused by other users.

There also exists an option (not displayed in the default configuration) to remove the user from the organizations system. This is a special functionality used to integrate (using a UserDataSource) with existing authorization systems and should remove all privileges connected with the user when he leaves the organization.

Reactivate Tokens

The reactivate token page unrevokes ordinary or consultant cards and optionally used to integrate ToLiMa into existing authorization systems that supports reactivation of cards.

It is usually used when a user has had a spare card issued but finds his ordinary card and wants to use that again. What actually happens is that the temporary card is revoked, the ordinary card gets unrevoked (it is put on hold when the temporary card is issued) and a signal is sent to the authorization system that the inserted card is the one that should be used.



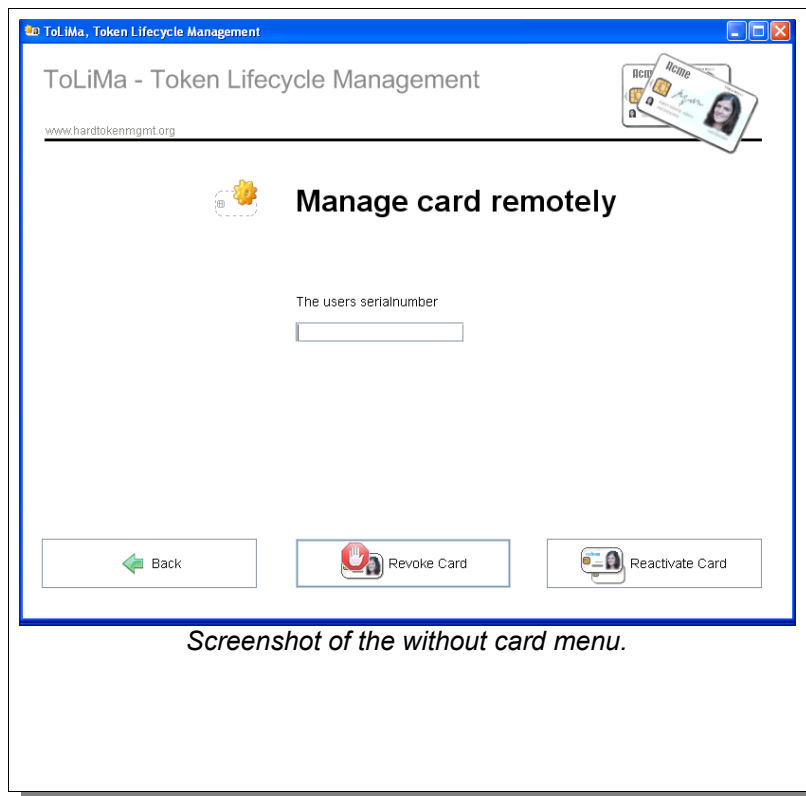
Administrator Actions without the Card

There are two actions that can be done by an administrator without having the physical card at hand.

One is to remotely block or revoke a card, this is usually done if a card has been lost. All that needs to be done is to enter the unique ID of the user and all the user's active tokens will be fetched from the database. It is then possible for the administrator to select the requested card and revoke it.

The other action is to reactivate a card. This is used if a user finds his ordinary card and calls the administrator that he wants it activated in the authorization system instead of the temporary one. What actually happens is that the certificates on the ordinary card that are temporarily revoked get unrevoked and optionally a signal is sent to the authorization systems about which certificate that actually should be used. This action works in the same way, the user unique ID is entered and all cards that are "on hold" are fetched from

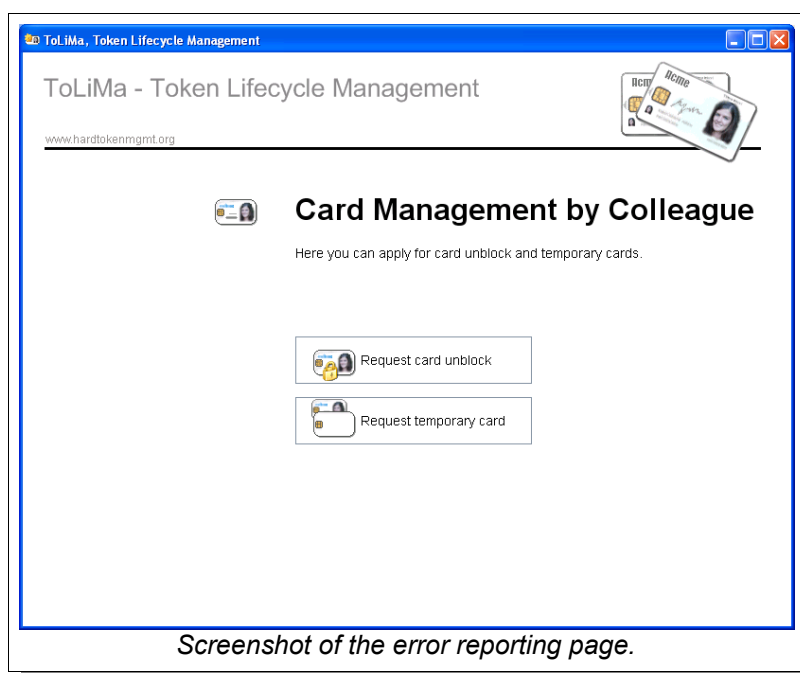
database.



Non-administrator Actions

There also exists functionality in ToLiMa for regular users that doesn't have administrative privileges. This is useful for 24/7 operations where a card administrator isn't always at hand.

Regular users have two operations to choose from, one is to unlock the PIN of locked cards, the other one is to generate spare cards if a users regular card have broken or been forgotten at home.



Regular users cannot perform actions by themselves, instead is a request sent to EJBCA for approval by some approval administrator. Technically it works in this way:

- First must the user that have a problem find a colleague with a working card and have him to log-in to the application. Since he probably won't have administrative privileges he will see the simplified menu below.
- Locked cards are first checked that they actually are locked. When requesting a spare card must the user enter his user id and name (if user data is fetched from a central location is only the user id required).
- Then is a request sent for approval in EJBCA which is in it's turn sends an email to the approval administrator for review. Usually is the central help desk or support unit used as approval administrators.
- The colleague is asked to manually call the approval administrator to verify his identity (and to speed up the process) and state the approval request id.
- The approval administrator will then click on a supplied link in the approval request email to be able to review the data. In the web page that follows he can choose to approve or reject the request.
- If the request is rejected cannot the user request for a new unlock or spare card for 8 hours (in the default configuration).
- If the request is approved will the colleague be able to unlock the users card or issue a spare card with 10 days (fixed) validity.

The ToLiMa application can be closed during the waiting but an approval is only valid for eight hours (in the default configuration) before a new approval request have to be generated.

MS SmartCard Logon Guide



Introduction

This document describes how to setup SmartCard Logon in a Windows environment to allow users to logon with a Smartcard and PIN-code instead of username and password.

Enabling SmartCard Logon

Prerequisites

Before enabling SCL the installation of SmartCard 2.0 image must be complete. This instruction assumes that the the image can be accessed from any machine and at least one card in addition to the initial administrator card has been personalized. The initial administrator card is used for all operations in the EJBCA Administration GUI.

The Domain Controller used in this setup is a Windows 2003 Server and the client machine is running Windows XP Pro. The domain name used is "ad.company.com", the DNS of the SmartCard2.0 image is mapped to both "smartcard20.demo" and "ca.company.com".

The DNS entries can be changed to fit your organization, just replace the names when following the documentation.

Request a Domain Controller Certificate

To be able to accept logon requests from clients the Domain Controller has to be able to identify itself to those clients. A Domain Controller Certificate is used for this purpose.

- Logon to the DC as Administrator, download the helper scripts from <http://smartcard20.demo/SCLScripts.zip> and unpack them.
- Run the script "1. GenerateDCCertRequest.vbs" and get a visual confirmation "Done!". This script produces "DomainControllerCertRequest-<hostname>.req" containing the request and a "DomainControllerInfo-<hostname>.txt".
- Use the initial administrator card from any machine to logon to the EJBCA Admin GUI <http://smartcard20.demo:8443/ejbca/adminweb/> and "Add End Entity" as shown below. The one-time password is set to "foo123" and CN, DNS and Globally Unique Id are all from the "DomainControllerInfo-<hostname>.txt"-file generated in the last step.

Add End Entity

| | | |
|--|----------------------------------|-------------------------------------|
| End Entity Profile | EEP_DomainController ▾ | Required |
| Username | DomainController-01 | <input checked="" type="checkbox"/> |
| Password | ●●●●●● | <input checked="" type="checkbox"/> |
| Confirm Password | ●●●●●● | |
| Batch generation (clear text pwd storage) | <input type="checkbox"/> | |
| Subject DN Fields | | |
| CN, Common Name | COMPANY-01 | <input checked="" type="checkbox"/> |
| O, Organization | Company | <input checked="" type="checkbox"/> |
| Subject Alternative Name Fields | | |
| DNS Name | company-01.ad.company.com | <input checked="" type="checkbox"/> |
| Globally Unique Id | 152fdda55294224da0abd5a738d07ccd | <input checked="" type="checkbox"/> |
| Certificate Profile | CP_MSDomainController ▾ | <input checked="" type="checkbox"/> |
| CA | MicrosoftCA ▾ | <input checked="" type="checkbox"/> |
| Token | User Generated ▾ | <input checked="" type="checkbox"/> |
| <input type="button" value="Add End Entity"/> <input type="button" value="Reset"/> | | |

- Logon to the Domain Controller again (if needed) and fetch the Domain Controller Certificate from EJBCA Public Web pages
<https://smartcard20.demo:8442/ejbca/enrol/server.jsp>.
 - Enter username "DomainController-01"
 - Enter password "foo123"
 - Paste the content of "DomainControllerCertRequest-<hostname>.req" into the text-area
 - Select PKCS7
 - Click OK
 - Save the resulting page as "DomainControllerCertRequest-<hostname>.p7b".

Enroll

Username

Password

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDVTCCAr4CAQAwADCBnzANBgkqhkiG9w0BAQEFAA0BjQAwgYkCgYEAxZ9W07he
qOLztZb1v774iPbrCgt6bVOIjoJfe9OS9AI9xkgJhNRWK+UvGaR6bIph6a+q7a//
BMuD8hCCy7WSCuSn6wTCQ4yRY+bfft8OB+fi3JAogf7iG+XxQgREjPM4jP2S+bXz
Cs1gkupnF9labhBY4PeH2Rt6AnPB91rzwEUCAwEAAAaCCAhMwGgYKKwYBBAGCNwOC
AzEMFgo1LjIuMzc5MC4yMEwGCSsGAQQBgjcVFDE/MDOCAQEMGNvbXBhbnktMDEu
YWQuY29tcGFueS5jb20MEEFEXEFkbWluaXN0cmF0b3IMC2N1cnRyZXEuZXh1MIGm
BgkqhkiG9w0BCQ4xgZgwZUwHQYDVRO0BBYEFJhRb+7jUh5BoSTi7guQCp8EEAms
MEgGA1UdEQEB/wQ+MDyCGWNvbXBhbnktMDEuYWQuY29tcGFueS5jb22gHwYJKwYB
BAGCNxkBoBIEEBUv3aVS1CJNoKvVpzjQfMOWHQYDVRO1BBywFAYIKwYBBQUHAWEG
CCsGAQUFBwMCMAsGA1UdDwQEAwIFoDCB/QYKKwYBBAGCNwOCAjGB7jCB6wIBAR5a
AEOAaQBjAHIAbwBzAG8AZgBOACAAUgBTAEEAIABTAEMAAaABhAG4AbgBlAGwAIABD
AHIaEQBwAHQAbwBnAHIAYQBwAGgAaQBjACAAUABYAG8AdgBpAGQAZQByA4GJAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Result type

Install the Domain Controller Certificate

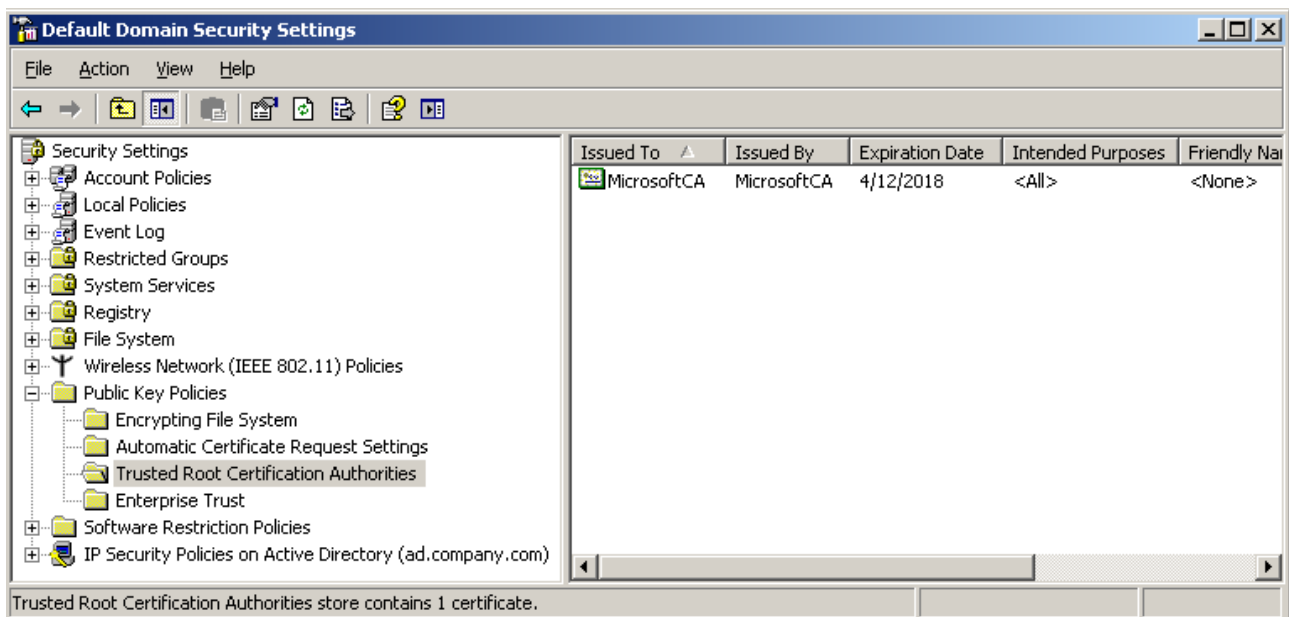
- Run the script “2. InstallDomainControllerCert.vbs” on the Domain Controller and select the "DomainControllerCertRequest-<hostname>.p7b" file. You will get the chance to verify that a certificate was installed in the last pop-up.

Install the MSDomain CA Certificate

- On the DC, browse to http://smartcard20.demo:8080/ejbca/retrieve/ca_certs.jsp and download the Netscape/Mozilla version of the the MSDomainCA certificate. The file will be called “certdist.cer” by default.
- Run the script “3. ImportCACertToNTAuthStore.vbs” and select the downloaded “certdist.cer”-file. You will get the chance to verify that a certificate was installed in the last pop-up.

Propagate the MSDomainCA Certificate to all Clients

- You can add the CA certificate to all client machines by adding it to the Domain Security Policy. On the Domain Controller: Start → Administrative Tools → Domain Security Policy → Public Key Policies → Trusted Root Certification Authorities → Right-click and choose “Import” → Next → Choose the CA certificate in “File to Import” → Next → Next → Finish



The cert is now propagated to all clients within 8 hours. This can be sped up by running “gpupdate /force” on relevant client machines connected to the AD.

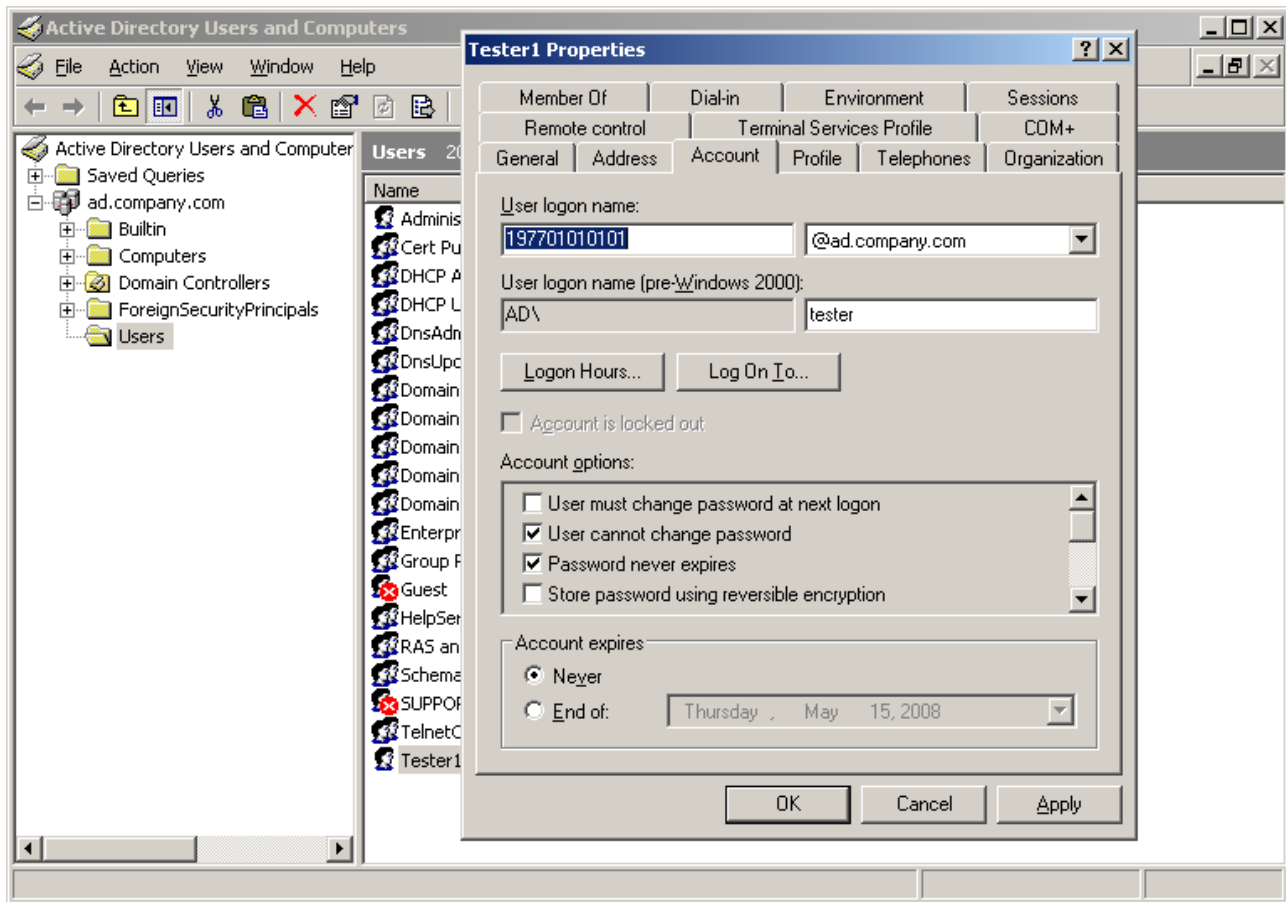
- Reboot the AD.

Install CSP on Client Machine

- Surf to <http://smartcard20.demo/website/smartcard20-getting-started.html> and download, unpack and install NetId. Also install any drivers for your smartcard reader.

Verify Setup

- From the client, make sure that the CA-machine is reachable so CRLs can be downloaded (<http://smartcard20.demo:8080/ejbca/>).
- Verify that NetId can read a personalized card and that the certificate issued by Microsoft CA looks ok. (An absence of warnings is ok.)
- Looking at the details in the certificate under SubjectAltname, the principal name is shown as 197701010101@ad.company.com. This is what Windows will look for in the AD during login and an account's “User logon name” must match this.



Logon with SmartCard

Insert the card in the card reader at the logon-screen. You should be prompted for the authentication PIN and, if entered correctly, allowed to logon.

PDF Signing Guide



Introduction

This section describes how to perform client side PDF signing using Adobe Acrobat in a Windows environment.

Generating signed document can be done for different reasons and in different ways. The most common reason is for integrity and authentication meaning that the recipient of the signed document can, through verification, be assured that the document has not been altered and that it originates from the expected source.

An organization that wishes to utilize these security features can choose between server generated signatures or client signatures.

Client signatures

Client signatures are created on the client where the document is authored. The client signature is initiated by the author of the document and the signature on the document identifies and authenticates the author. This also means that the author later on can not deny that he/she wrote the document, because the signature guarantees that the document hasn't been altered after being signed. This is the most common signature requirement and is the method described in this document.

Server signatures

Server generated signatures are used when a document is signed as originating from an organizational entity. A recipient can verify that the document originates from the organization but can not authenticate the person who created the document. This is many times a desired feature. Server signatures can be created by a signing server, such as the SignServer (<http://www.signserver.org/>). Server signatures are out of the scope of this document.

Enabling PDF Signing

Prerequisites

Before enabling PDF Signing the installation of SmartCard 2.0 image must be completed. This instruction assumes that the image can be accessed from any machine and at least one card in addition to the initial administrator card has been personalized. The additional user card will be used to generate signatures on PDF documents.

To sign PDF documents using this Guide, you need to install Adobe Acrobat Professional, version 7 or later. This guide will use version 7 of the software, so if you are using another version some choices in the menus may be slightly different. The concepts will be the same, so you should be able to find the functions.

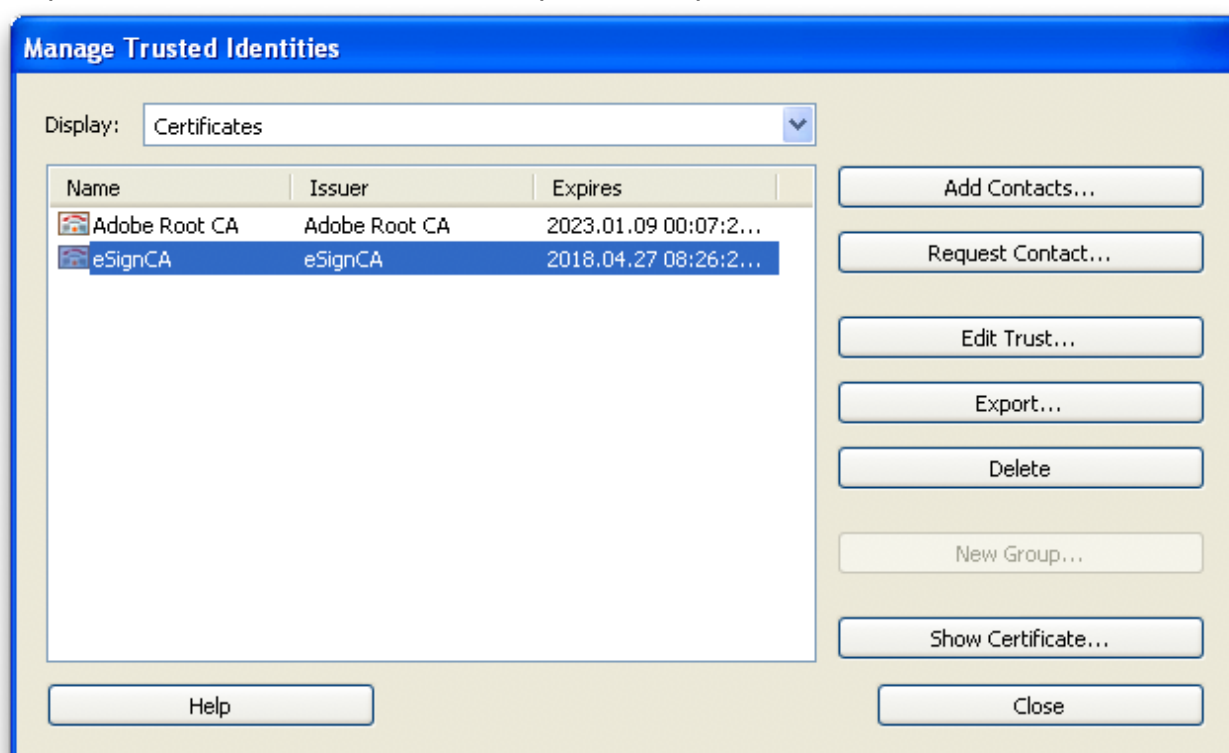
The PDF signing should be performed on a machine with NetID and a card reader installed. It is suggested to use the same machine where SmartCard2.0 is used to create cards.

Install the CA certificate in Adobe Acrobat

To fully verify a signature the trusted Root certificate must be installed in Adobe. To download the Root CA certificate go to https://smartcard20.demo:8442/ejbca/retrieve/ca_certs.jsp and on eSignCA right click the CA-link under “For Internet Explorer” and choose “Save as”. Change the extension on the file to “.cer”.

Import the certificate in the menu *Advanced->Trusted Identities*. Click *Add Contacts*, browse to the Root CA certificate file and import it. Then select the newly imported certificate in the list and click *Edit Trust*. Select the check boxes *Signatures and as a trusted root* and *Certified documents*.

The picture shown below is after the import is complete.



Signing documents

Open up Adobe Acrobat and open a PDF document, for example this document.

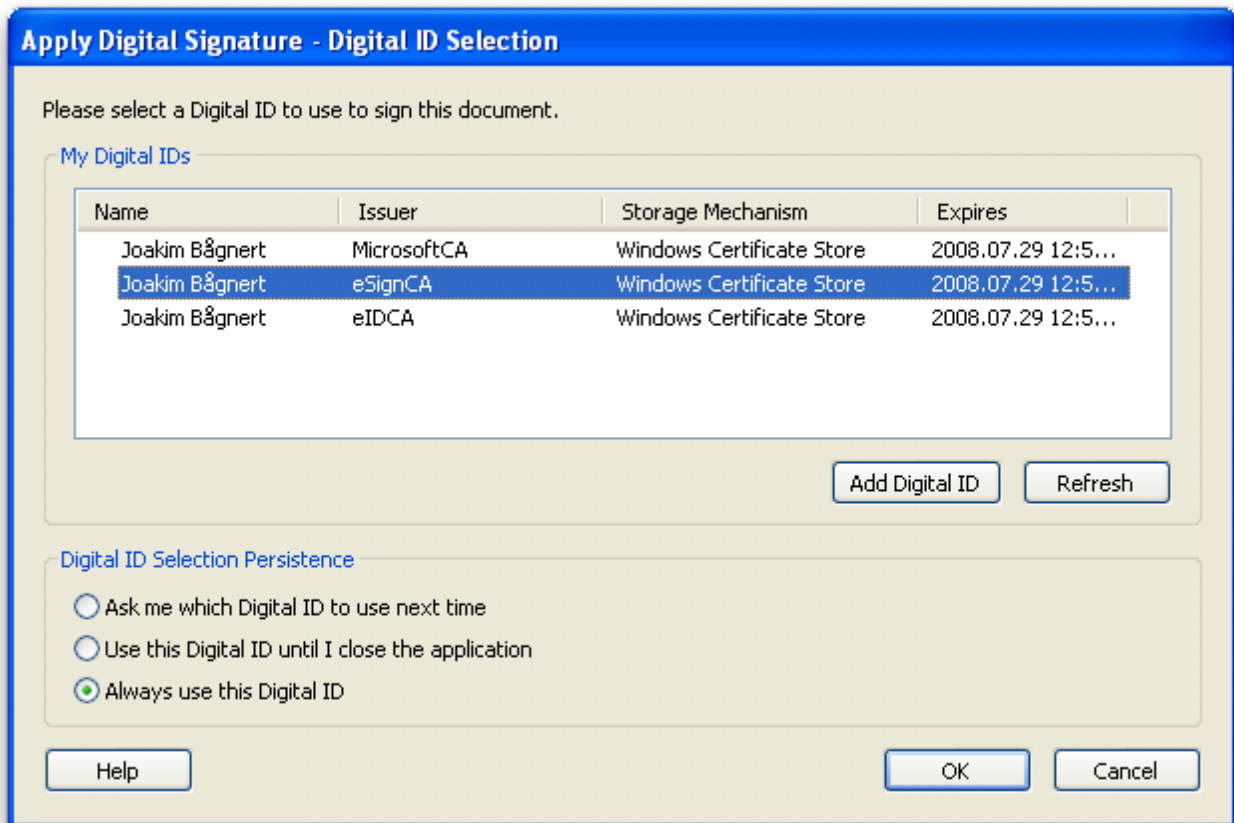
Insert the users smart card in the card reader and click the *Sign* icon in the toolbar. Select *Sign this Document*.

Read the information in the pop-up and click *Continue Signing*.

Select *Create a new signature field to sign* and click *Next*.

Click *OK* and draw a rectangular signature area in a white area in the document.

You are now presented with a dialog with certificates. Use one to sign the document.



This is where Acrobat makes it difficult for the user. It displays all certificates available in the machine and lets the user try to make a good selection, without displaying enough information. In this case we know that the *eSignCA* issues the certificate we want to use, so we can select that.

Click *OK*.

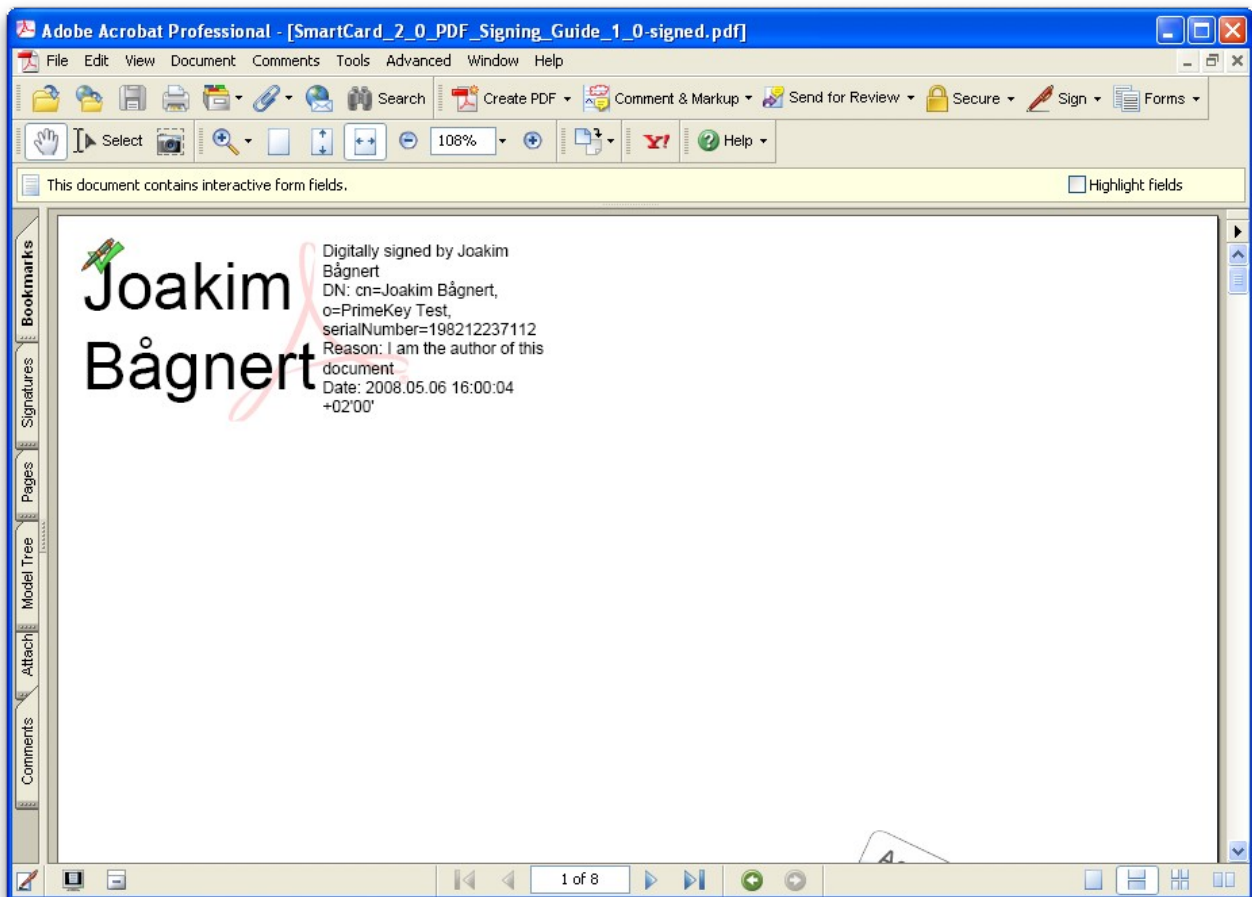
Select *I am the author of this document* in the next screen (you can select anything you want here), then click *Sign and Save As*, and save the document with a new name.

You will be asked for your **signature PIN**. After this you can see the signature field in the document.



Verifying signed documents

Verifying signed documents are done automatically when opening a signed PDF using Adobe Acrobat or Adobe Reader. When a document is signed the panel *Signatures* is shown on the left. By clicking in this panel you can get full information about the signer of the document and the verification steps performed. You can also get information by clicking on the signature field in the document.



If you click the signed picture you get the picture below where you can get more information about the signature.

Appendix A, References and Links

Contacts

Integrator

<http://www.logica.se>

Developers of EJBCA and ToLiMa projects:

<http://www.primekey.se>

Developers of NetID client:

<http://www.secmaker.se>

More Documentation

ToLiMa project Main Web Site:

<http://www.hardtokenmgmt.org>

ToLiMa Flash Demo:

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

HardTokenMgmt Framework Developers Guide:

<http://www.hardtokenmgmt.org/developersguide.html>

EJBCA Main Web Site:

<http://www.ejbca.org>

Tutorials for EJBCA administration:

<http://wiki.ejbca.org/admintutorials>

Documentation about developing a customized UserDataSource:

<http://www.ejbca.org/manual.html#Framework%20for%20External%20User%20Data%20Sources>

Documentation about developing a customized Publisher:

<http://www.ejbca.org/manual.html#Custom%20publishers>

