

Card Administrators Guide

SmartCard 2.0



1.2

Table of Contents

Introduction.....	3
Who should read this document.....	3
Terms explained.....	3
Crash Course in SmartCard Management.	5
About ToLiMa.....	5
What is a SmartCard?.....	5
Why two PIN codes?.....	5
What is cryptographic keys?.....	6
What is a certificate?.....	6
What does revocation mean?.....	6
Managing SmartCards with ToLiMa.....	7
Starting the application.....	7
The Login Page.....	7
The Main Page.....	8
Generating Tokens (SmartCards).....	9
Renew Token.....	10
Unblock Token.....	11
Viewing Tokens.....	11
The different card types.....	12
The different certificates.....	12
Revoke and Clean Cards.....	13
Reactivate Card.....	13
Administrator Actions without the Card.....	14
Non-administrator Actions.....	14

Introduction

This document describes the basics of SmartCard management and how to operate the ToLiMa (Token Lifecycle Management) application from a card administrators point-of-view. Card Administrators are usually designated people administrating identity cards within an organization.

This document is divided into two sections; basics of SmartCard management and the ToLiMa application.

'SmartCard 2.0' is the name of a minimal configuration of ToLiMa that is easy to set up and evaluate in an organization.

Who should read this document

The intended audience are card administrators that want instructions and information about how to manage SmartCards using the ToLiMa (SmartCard 2.0) application.

Terms explained

Here are some of the common terms used when managing SmartCards that can be good to know. Some of the terms will be explained further in the next section.

<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.
SmartCard	A physical token that contains the user's private keys. The keys can never leave the card or be copied by someone else.
Private Key	A 'Private Key' can be seen as a unique secret code of a user. With this secret he can be perform cryptographic operations, used for example when authenticating (workstation log in), electronic signatures or encrypting documents.
PIN	A PIN code protects Private Keys on the SmartCard. The user needs to enter this

	<p>code in order to use the Private Keys. This guarantees that only the user can have access to the keys.</p> <p>A PIN code is usually a password of 4-8 characters or digits.</p> <p>A SmartCard usually have two PIN codes, one for authentication and encryption (also called 'basic PIN' or 'identification PIN' and the other is used for electronic signatures called 'Signature PIN'.</p>
Certificate	<p>A certificate is used to connect a user's private key with the identity of the user and is used to prove to other users that the key really belongs to that person.</p> <p>A certificate usually contains information that identifies the user such as a unique name (called DN or Distinguished Name) and some public information connected to the private key. The certificate itself isn't sensitive.</p> <p>A certificate is created by a 'Certificate Authority' which can be seen as a trusted third party.</p>
CA	<p>"Certificate Authority". A CA issues certificates to, and vouches for the authenticity of the users.</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.</p>
DN	<p>"Distinguished Name", Name used in a certificates to uniquely identity the user. Example of a DN is "CN=Pelle Petterson,SN=1234,O=Acme inc,C=SE" where CN stands for Common Name, SN for serial number (usually employment number or something similar), O for organization and C for country.</p>

Crash Course in SmartCard Management.

About ToLiMa

ToLiMa stands for Token Lifecycle Management and is a SmartCard management application. It has been developed with customers having a long experience of smart card usage and is adapted to their requirements of a functional system.

The name SmartCard 2.0 is a simplified configuration of ToLiMa that is easy to get started with and is used for demonstration and proof of concept purposes.

What is a SmartCard?

A SmartCard is basically a physical token that contains the user's private keys. The keys can never leave the card or be copied by anyone. The keys are protected by a PIN code required for access to a private key. This results in something called a “two-factor authentication”; something you have (the SmartCard) combined with something you know (the PIN). This is more secure than just “one-factor authentication”, which usually is just something you know; a username and a password. These credentials can easily be copied without the user's knowledge.

Usually there are two keys stored on the card used for different purposes, one is for authentication and the other for electronic signatures. With authentication means either to log on to a workstation or to the Intranet on the web. Electronic signatures can be used in PDF documents or forms instead of a handmade signature.

Why two PIN codes?

It is common that a SmartCard has two PIN codes, one that protects the authentication key (often called 'basic PIN' or 'identification PIN') and another one that protects the signature key (called 'signature PIN').

The reason for two codes is that they behave slightly differently. Once the correct password is entered for the basic PIN its protected key will be unlocked until the user removes the card from the card reader. The user shouldn't be forced to enter his code more than once to identify to different applications. The signature PIN however is unlocked for one signature only, then it's locked again. This to ensure that a user doesn't sign any document or email by mistake or without even knowing it.

If a user enters the wrong PIN three times or more the PIN will be blocked. This protects the user's identity in case of theft. In case the card is blocked the user must contact one of the card administrators and identify himself before the card administrator can help the user and unblock the card.

The basic PIN and signature PIN are completely separate, if one PIN is blocked the other might still have three attempts left.

What is cryptographic keys?

A 'Private Key' can be seen as a unique secret code of a user. With this secret he can perform cryptographic operations, used for example when authenticating (workstation log in), electronic signatures or encrypting documents. This key is protected in the SmartCard and cannot be copied.

A 'Private Key' also have a matching public part that is not sensitive and is kept in a certificate.

What is a certificate?

A certificate contains a matching public part of the user's key combined with a unique name of the user and some information of what is allowed to do with the key.

A certificate can be seen as an electronic identity card that is used to prove that the user really is the one he says he is.

Certificates are generated by something called a 'Certificate Authority' or 'CA' which can be seen as a trusted third party. This means that whoever trust this CA can rely on the correctness in the information stored in the certificate. The ToLiMa application is connected to such a CA and whenever a new SmartCard is generated is the CA involved issuing the certificates that is placed on the cards.

Each card have three certificates, two are used for authentication, were one of them is a general authentication certificate called 'eID' and the other is a Microsoft specific certificate used when logging on a Windows workstation. The later certificate is called 'MS log on'. The third and last is called 'eSign' certificate used for digital signature.

To avoid confusion about why there are three certificates and only two matching private keys is because the two authentication certificates share the same private key, they are only used for different purposes.

Certificates are only valid for a certain period of time, usually 5 years for ordinary employees. After that time the certificates have to be renewed by regenerating the SmartCard.

What does revocation mean?

SmartCards can be lost or stolen before the validity of the card expires. This event have to be reported to the CA that the certificates stored on that card cannot be trusted any more. This is called to revoke a certificate.

The CA will then periodically issue a list of all the certificates that isn't valid any more to relying parties. This list is called a CRL or Certificate Revocation List.

There are two types or revocations, one is to permanently revoke a certificate and the other to temporary revoke, called "on hold". The later one is sometime used when a user have forgotten his card at home and a temporary card is issued during the workday.

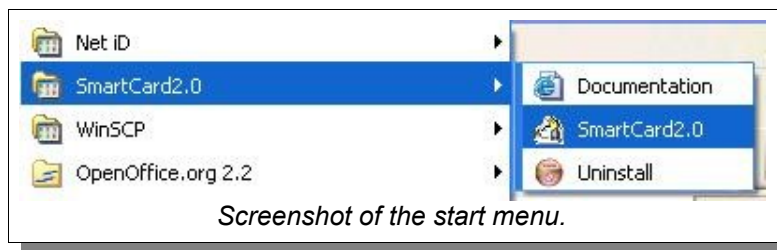
Managing SmartCards with ToLiMa

This section will give the details of operating the ToLiMa application. How it works and what the options are.

Starting the application

After installation should ToLiMa be a part of the Windows start menu. Under the SmartCard2.0 tab, click on the option also called SmartCard2.0 to start the application.

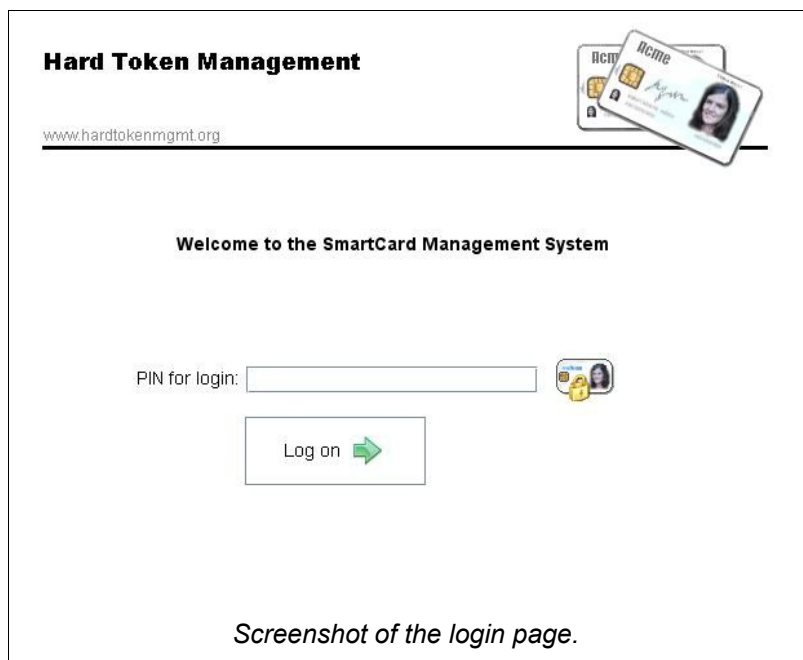
Important! Before you start the application, be sure that you have two card readers installed on the workstation, one for your card and the other for the card to process.



The Login Page

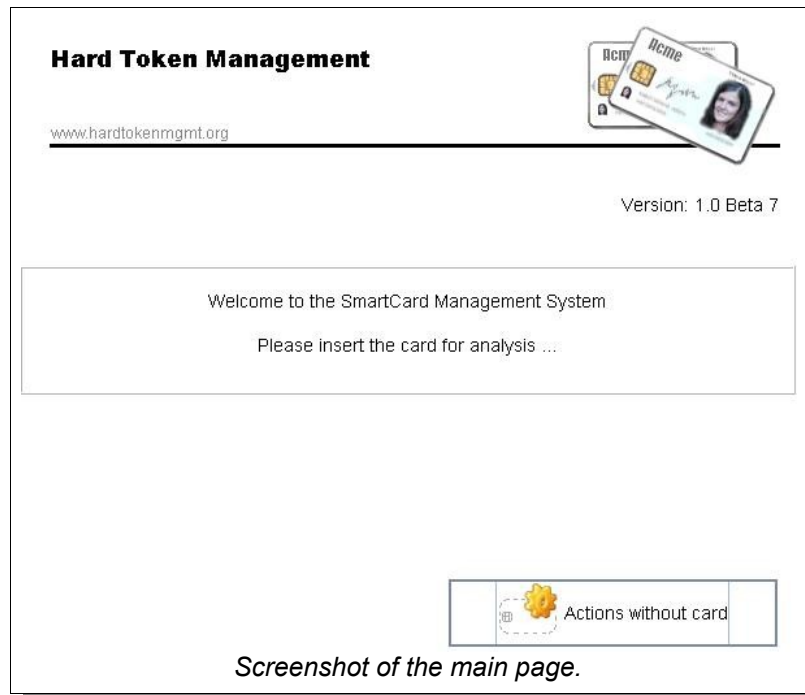
First you will be prompted to insert your own SmartCard to identify yourself against the application then enter your basic PIN used for login.

Remember that you only have three attempts to unlock the PIN before it will get blocked.



The Main Page

After log-on is the main page displayed. This page will perform an analysis of what might be wrong with the card to process and redirect you to the page you most likely will use to make the card operationable again.



As soon as the processable card is inserted, the following analysis is done:

- If the card is empty or revoked it will redirect you to the 'Generate New Card' page.
- A card that is about to expire (default is less than 10 days) will lead to the "Renew Card" page.
- If the card is blocked it leads to the PIN unblock page.
- If the card is temporary revoked it leads to the reactivate page.
- If the card seems normal a simplified menu is displayed with the options to view the details, revoke and clean or reactivate a temporary revoked card.

There also exists a button that takes you to the "Actions without card" menu. In that menu it's possible to revoke cards that isn't physically at hand.

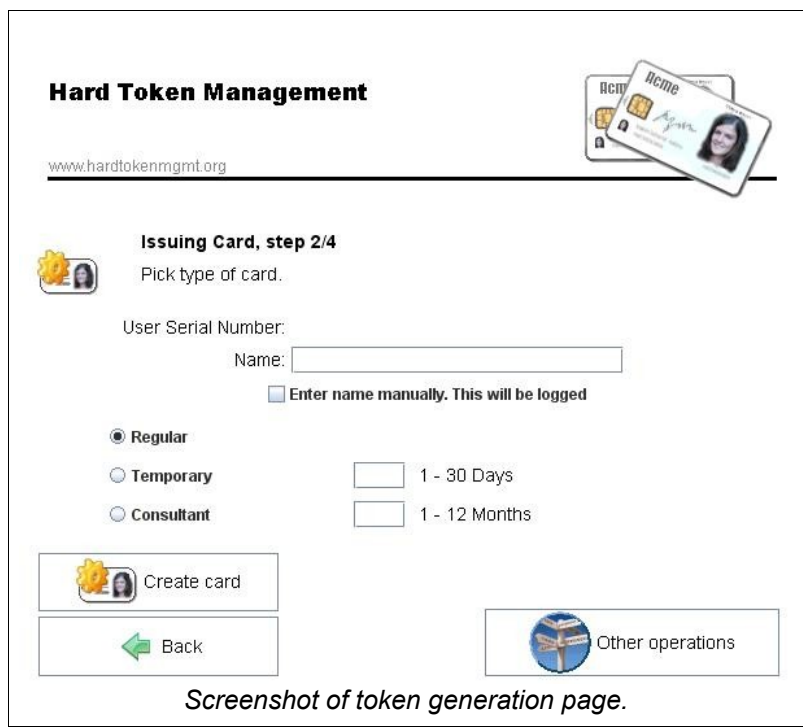
Generating Tokens (SmartCards)

For new employees or users that have lost their card and need a new one, either temporary or ordinary is the generate token page used. You will get to this page by inserting an empty or revoked card in the main page, but it is also possible through the 'Other Actions' menu displayed if the analysis suggest another action.

Generating a Token is done in four steps:

1. In the first page you are requested to enter a unique id of the user (usually an employment number). Then click on 'Create Card' to get to the next step.
2. In the next page you should enter the name of the user and select the type of card to issue. The card types 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.

Then click on 'Create Card' to continue.



Screenshot of token generation page.

3. In the third step is the actual token generation performed. The card is first initialized and the private keys generated on it and then three certificates are generated by the CA and placed on the card.

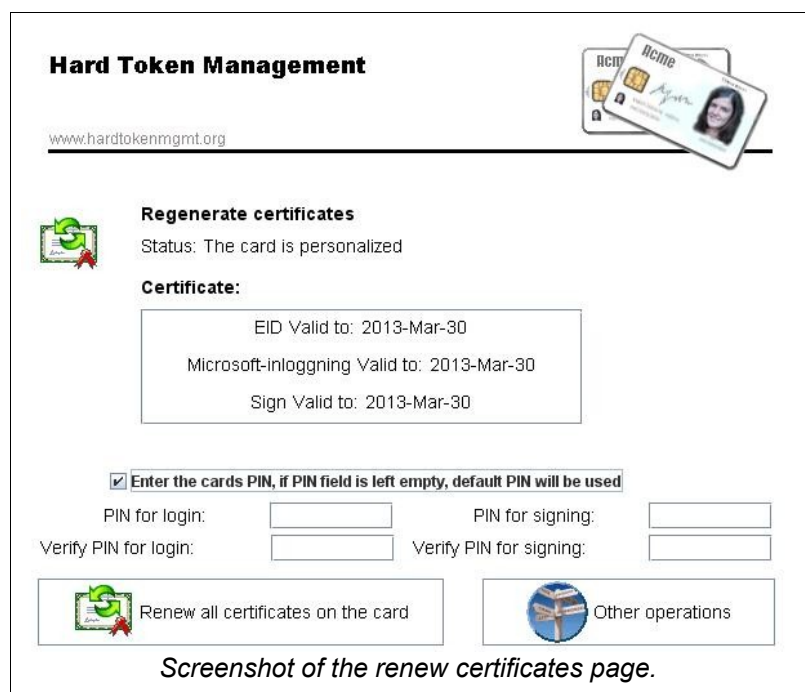
The users old cards will be revoked permanently if a new ordinary or consultant card is generated. Issuing a temporary card for the user will result in the old card getting temporarily revoked.

4. In the fourth and final step the card's new PIN codes are set and displayed for the user. In the default configuration the identification (also called basic) PIN is set to a static value that the user is supposed to change the first time the card is used and the signature PIN set to a random value.

Renew Token

The renew token page is displayed if a token is about to expire (with a shorter validity than 10 days). The page can also be accessed manually through the view token page.

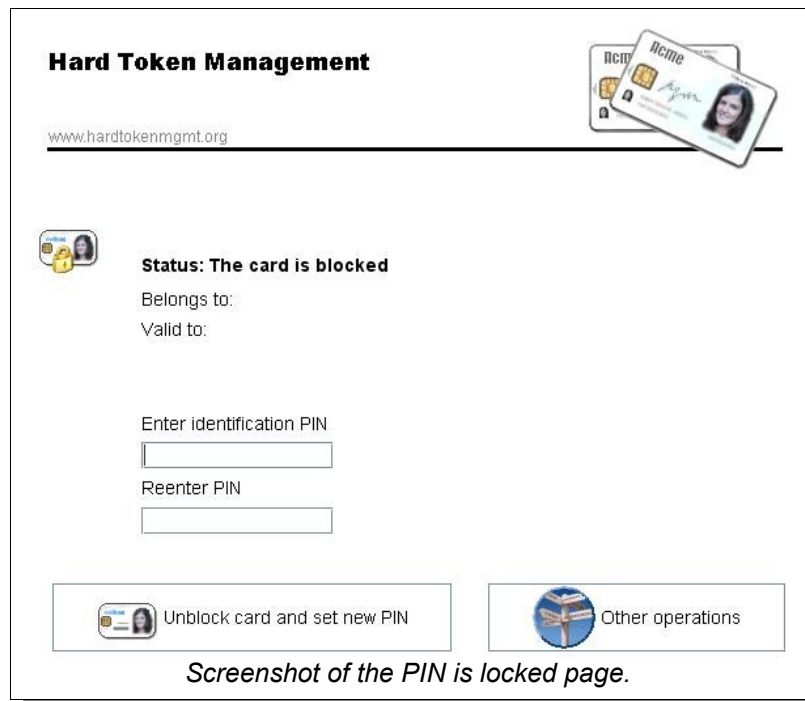
This option simply removes the certificates on the card and generates new ones with the same validity as the original. During this action the user have to enter the current PIN codes in order to renew the card. As an alternative it is possible to have the PINs generated in the same as when generating a new card.



Unblock Token

If the analyzer notices that one of the PINs is blocked, the unblock PIN page is displayed. The page lets the user enter his desired PIN and all that is left to do is to click on 'Unblock card and set new PIN' and the card will be ready to be used again.

This operation only unblocks one PIN at the time. If the user have blocked both PINs the operation have to be done twice, either by reinserting the card or by clicking on 'Other Actions' and then 'Unblock Card'.



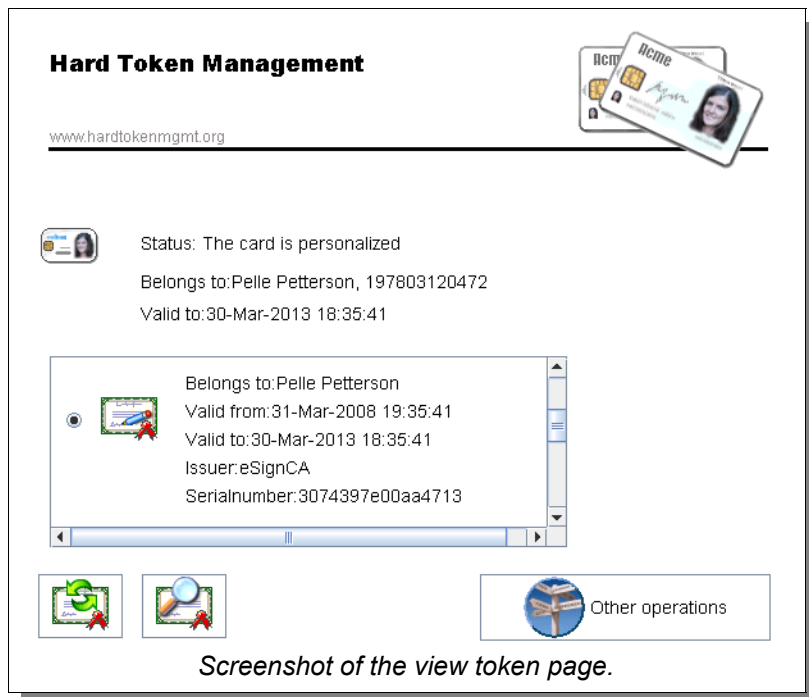
Screenshot of the PIN is locked page.

Viewing Tokens

In the view token page it is possible examine the certificates placed on the card.

In the main page is a list of details of the card and all its certificates. To view the details of a specific certificate select it and click on the 'view certificate' (the icon with a magnifying glass) button. You can also get to the renew certificates page from here.

The card have a different logotype depending on type of card. The certificates on the card also have different logotypes depending on usage. On the next page are the different logos explained for the available card types and certificates.



The different card types



Ordinary card with 5 years validity.



Temporary Card with 1 to 30 days validity'.



Consultant or project card with 1 to 12 months validity.

The different certificates



eID Certificate used for authentication.



eSign Certificate used for electronic signatures.

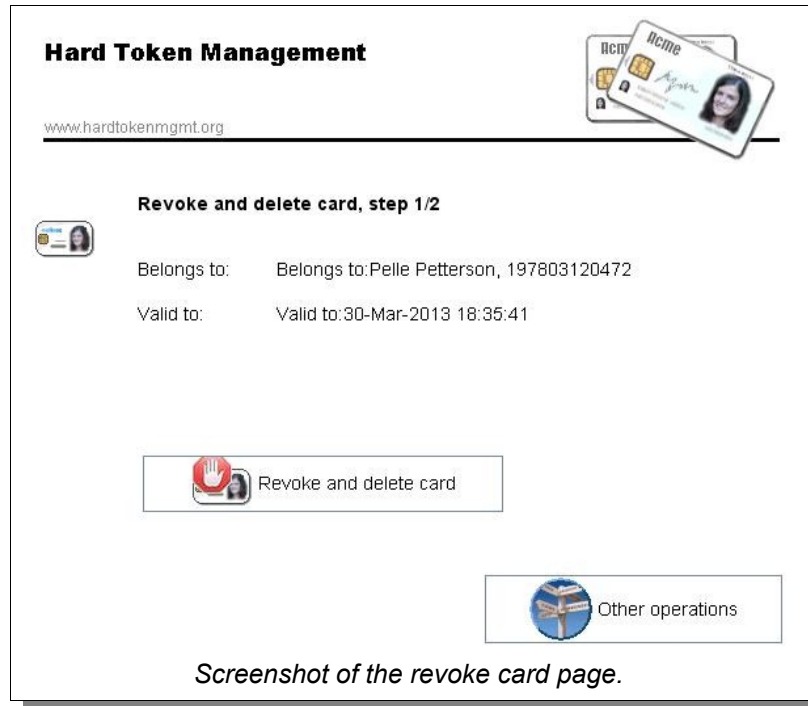


Microsoft Log on Certificate.

Revoke and Clean Cards

The revoke and clean card page revokes the certificates on the card permanently and cleans the card (removes the keys and certificates).

After doing this it's possible to reuse the card since no sensitive information no longer are stored on the card.



Screenshot of the revoke card page.

Reactivate Card

This option is used whenever a user got a token temporarily revoked and want it reactivated again. This is usually the case if a user one day have left his card at home and have received a temporary card, the next day he have got his ordinary card with him and want to start using that again. He will then also return his temporary card to the card administrator.

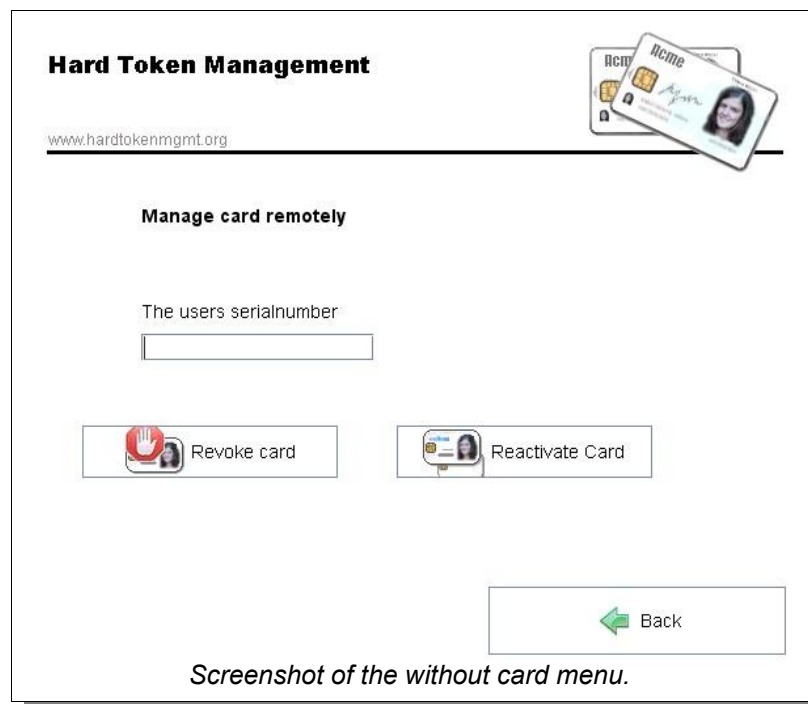
The page itself is simple with one main button, to reactivate the currently inserted card.

When a ordinary or consultant card is reactivated is the temporary card revoked permanently.

Administrator Actions without the Card

It is possible to revoke and reactivate cards that isn't physically available. Revoking this is usually done if a card have been lost and reactivating if a user have found hos ordinary card and want to be able to use it again and call in by telephone.

All that needs to be done is to enter the unique Id of the user and all the user's active (in the case of revoking) or temporary revoked (when reactivating) tokens will be fetched from database. It is then possible to select the requested card and click on the. 'Revoke Card' or 'Reactivate Card' button.



Non-administrator Actions

There also exists functionality in ToLiMa for regular users that doesn't have administrative privileges. This to ensure that the users can still use their SmartCards on off-business hours or when no card administrator is at hand.

The users have two operations to choose from, one is to unblock 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 SmartCard management actions by themselves, instead there is a request of what they want to do sent for approval to some approval administrator. Basically it works in this way:

- First must the user that have a problem with his card find a colleague with a working card and have him to log-in to the same application as the card administrator. Since he probably won't have administrative privileges he will see the simplified menu above.
- Blocked cards are first checked that they actually are locked. When requesting a spare card must the user enter his user id and name.
- Then is a request sent for approval which results in an e-mail sent 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 an approval request id.
- The approval administrator will then review the request, check that the information is correct and approve or reject the request.
- 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. The same time applies in the case the request is denied, the user and colleague cannot request again for 8 hours.

- After the request have been approved, the card is unblocked or a spare card is issued in the same way as if a card administrator would do it.

