



# Intercede MyID 7.1

## Betrifft Benutzer

**CRYPTAS it-Security GmbH**

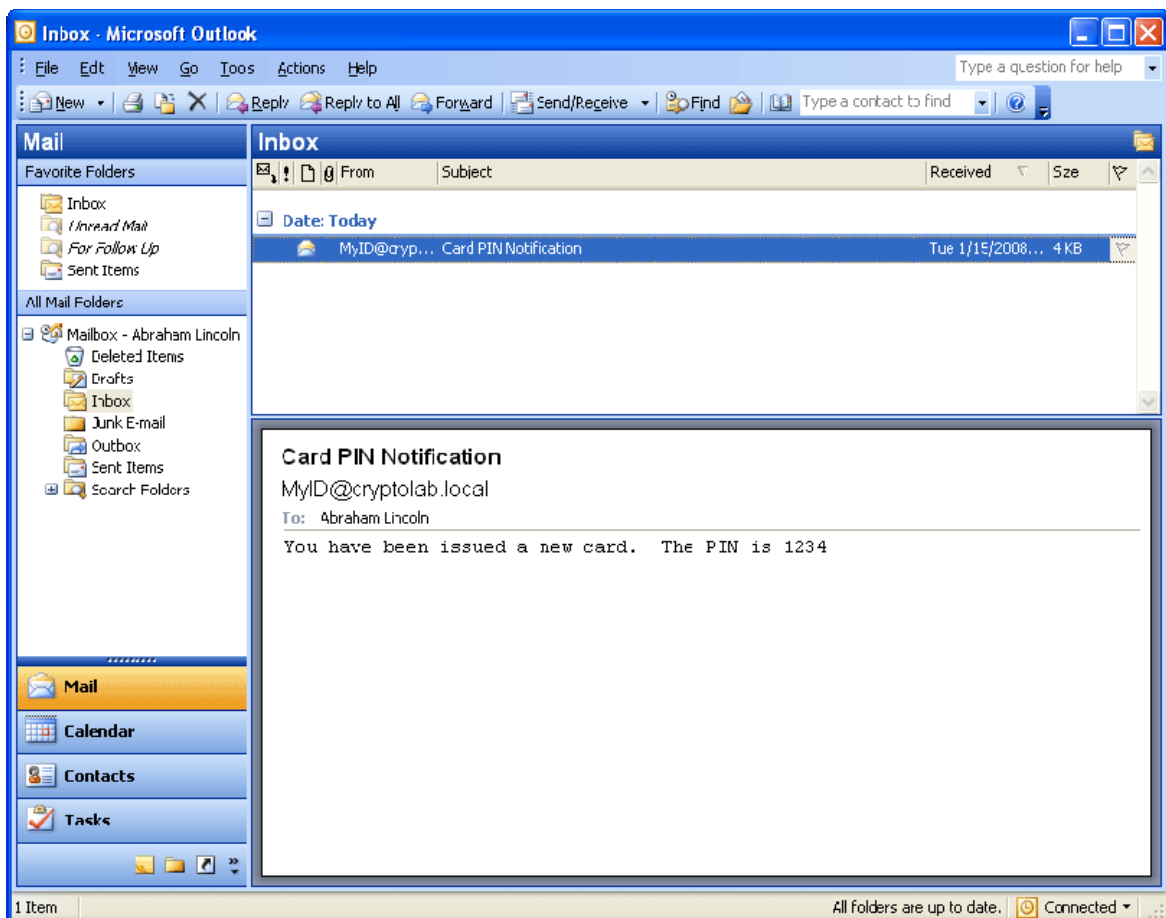
Modecenterstrasse 22/B2  
A-1030 Wien

[www.cryptoshop.com](http://www.cryptoshop.com)  
[www.cryptas.com](http://www.cryptas.com)

## Automatische Information der Benutzer

Intercede MyID verschickt (wenn es denn dazu konfiguriert wurde) automatische Verständigungen an alle betroffenen Benutzer. Dies betrifft die Ausstellung neuer Smartcards ebenso wie eine bevorstehende Erneuerung ablaufender Zertifikate und andere Vorgänge, die eine Information oder eine Interaktion des Benutzers erfordern.

In unserer Beispielininstallation beginnt die MyID und Smartcard Erfahrung unseres Testbenutzers „Abraham“ mit einer Email von MyID:



In unserer Beispielininstallation holt sich „Abraham“ nun seine neue Smartcard vom Administrator des Testlabors ab.

Selbstverständlich können die Inhalte und das Aussehen der Emailvorlagen den Bedürfnissen des Unternehmens angepasst werden. Beispielsweise wäre es hier hilfreich, außer des Hinweises auf die PIN auch noch das weitere Vorgehen des Benutzers zu beschreiben:

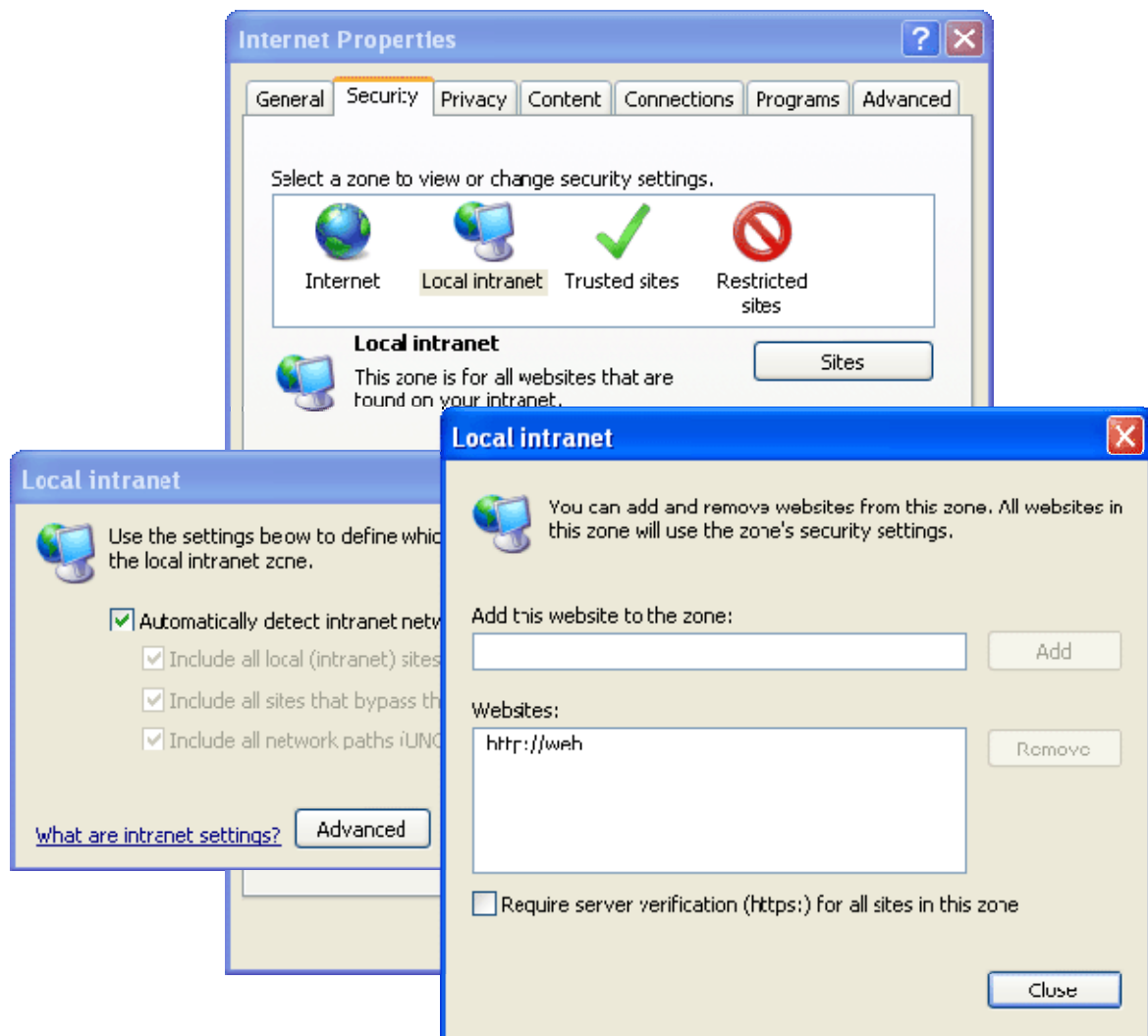
- Abzuholen bei XYZ.
- Öffnungszeiten von XX:00 Uhr bis YY:00 Uhr.
- Ändern sie nach dem ersten Anmelden umgehend Ihre PIN.
- Ein Link zur Security Management Console. ( <http://web/myID/us/> )

Tipp: „Corporate Identity“ ist meist eine „Chefsache“ und sollte unbedingt vorher mit den verantwortlichen Personen besprochen werden.

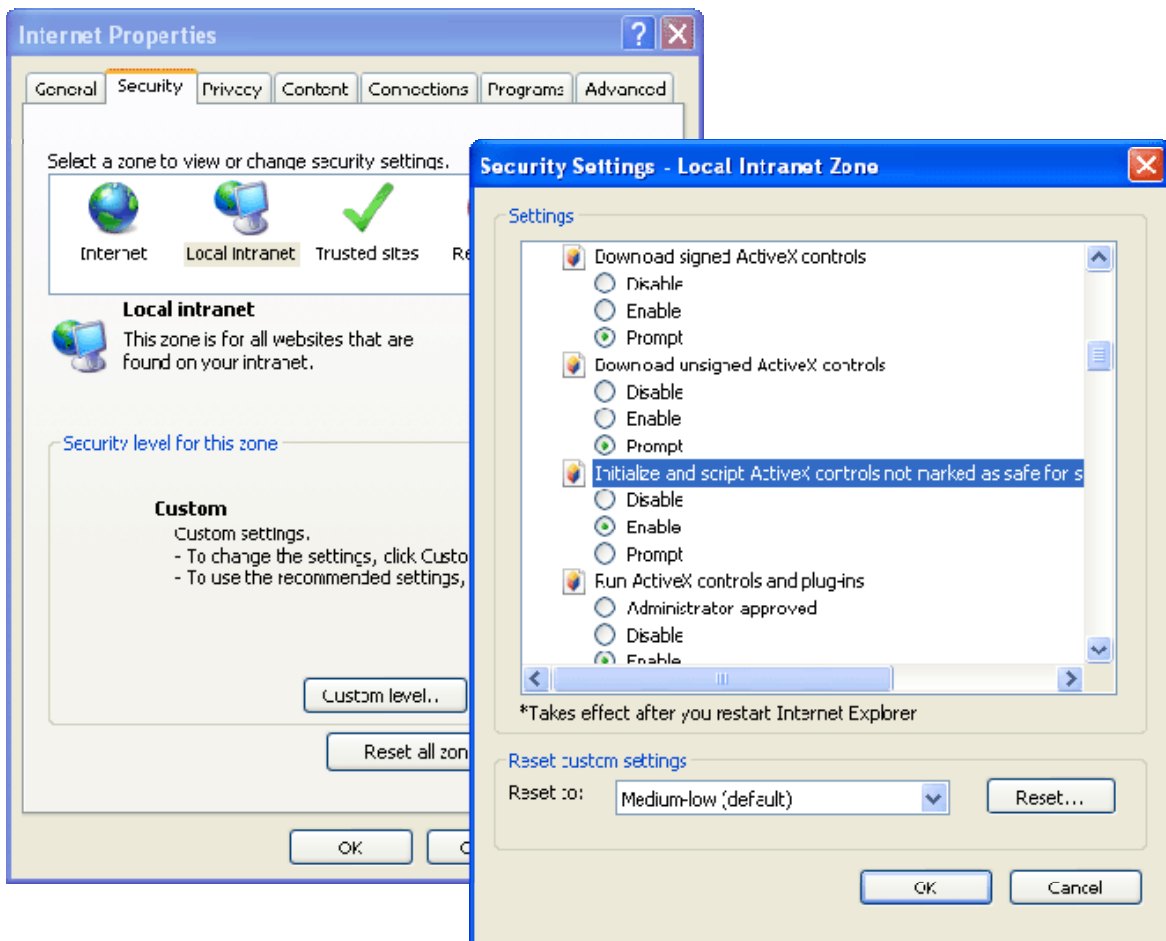
## Zugriff auf die Konsole durch den Benutzer

Wenn wir die MyID Security Console den Benutzern zugänglich machen wollen, so müssen wir sicherstellen, dass die Sicherheitseinstellungen von MS Internet Explorer nicht die Ausführung des ActiveX Clients verhindern.

Der Webserver, der das Webinterface von MyID anbietet muss sich in der Sicherheitszone „Local Intranet“ befinden.

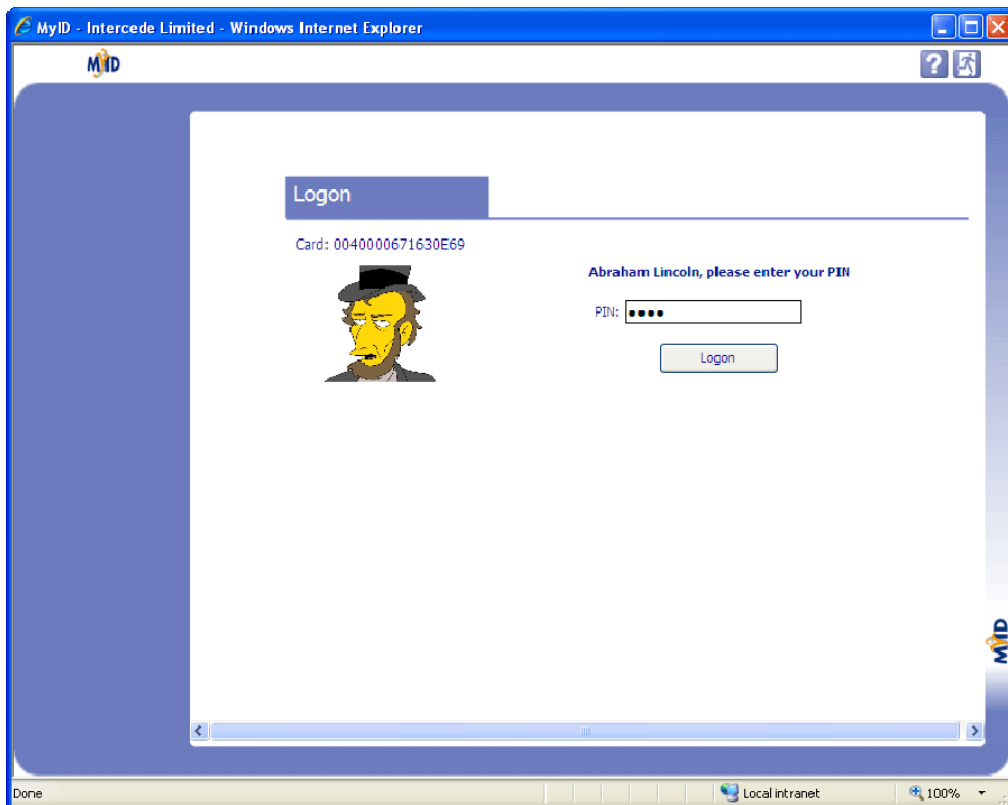


ActiveX Controls dürfen nicht eingeschränkt werden.

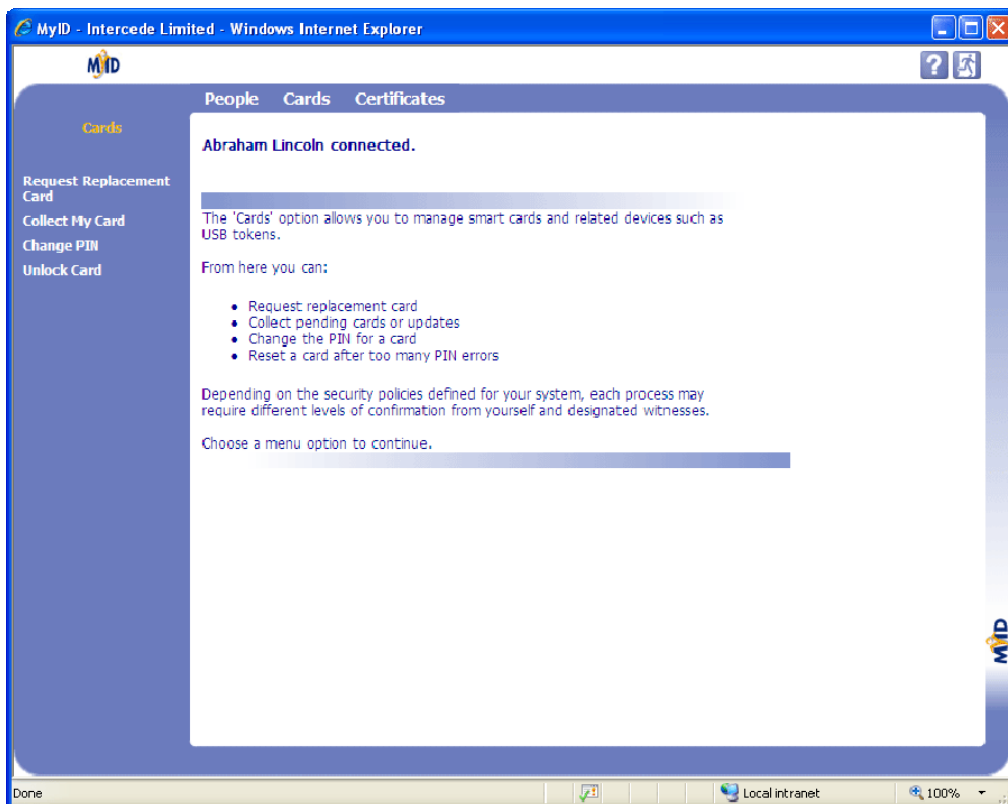


Tip: eine Einstellung im entsprechenden GPO des AD vereinfacht die Arbeit des Helpdesk enorm. Also rechtzeitig mit dem Domain Admin in Verbindung setzen.

Nun kann der Benutzer mit dem Link (<http://web/myID/us/>) auf die Security Management Console zugreifen.



Sich anmelden .....



... und auf die Applets zugreifen, die vom MyID Administrator der Rolle, welcher der Benutzer angehört, zugedacht wurden. Wir erinnern uns: im Konfigurationsteil haben wir Rollen erstellt und Berechtigungen zu Operationen erteilt. Dann haben wir dem Benutzer oder der Gruppe des Benutzers die Rollen zugeteilt. Diese Berechtigungen (in diesem Falle sehr eingeschränkte) sehen wir nun als Benutzer in unserer Konsole.

Wir wollen nun einige typische Fälle durchspielen, die unseren Testbenutzer „Abraham“ zustoßen können

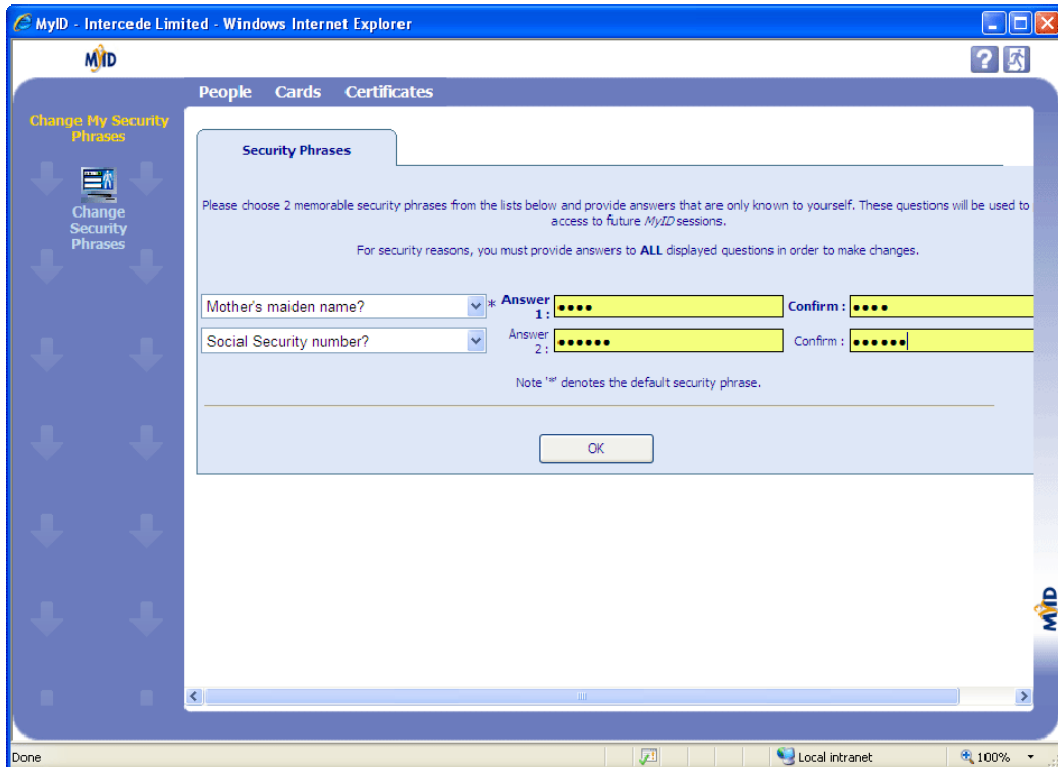
## Entsperren einer gesperrten Smartcard

Um einem Benutzer zu ermöglichen, seine gesperrte Smartcard selbst zu entsperren, muss er in der Lage sein, sich an MyID mit einer alternativen Methode zu authentisieren.

Dazu gibt es 2 Möglichkeiten:

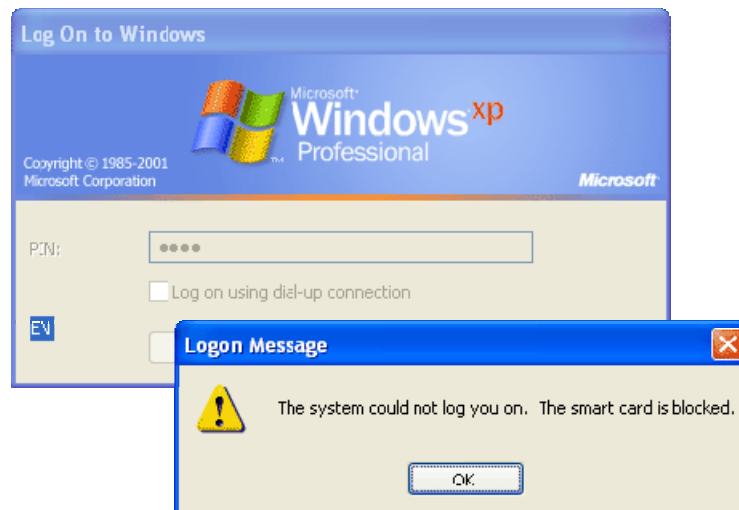
- 1.) Er nutzt die Windows Anmeldung.. Dazu müssen folgende Bedingungen erfüllt sein:
  - Am Webserver muss der anonyme Zugriff auf die Security Management Console deaktiviert sein. Weiters muss Integrated Windows Authentication aktiviert und Basic Authentication deaktiviert sein.
  - Die Richtlinien des Unternehmens müssen eine Ersatzanmeldung mittels Benutzername und Passwort erlauben. Das muss auch im Benutzerobjekt im AD so abgebildet sein.
- 2.) Er nutzt die alternative Anmeldung von Intercede MyID mittels Authentisierungsfragen. Dazu müssen wieder 2 Bedingungen erfüllt sein:
  - Er muss die Antworten von mindestens 2 Authentisierungsfragen vorbereitet und bereits in MyID eingetragen haben.
  - Er benötigt einen funktionierenden und angemeldeten Computer, der Zugriff auf die Webseite hat, etwa ein anonymes Terminal oder den Computer eines hilfsbereiten Kollegen.

Zum Vorbereiten der Authentisierungsfragen besucht der Benutzer bei Gelegenheit einmal die Webseite der Security Management Console ( <http://web/myID/us/> ) und meldet sich mit seiner Smartcard an.

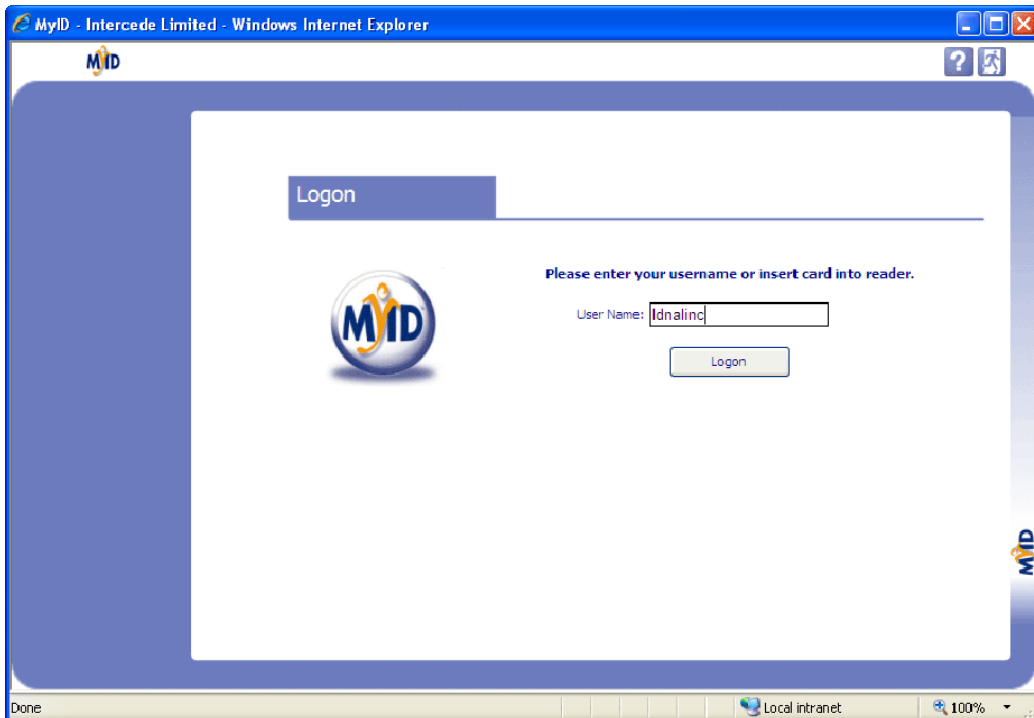


Hier wählt er sich 2 der vorbereiteten Fragen aus und gibt die nur ihm bekannten Antworten ein. Mit „ok“ speichert er die Antworten in der Datenbank ab.

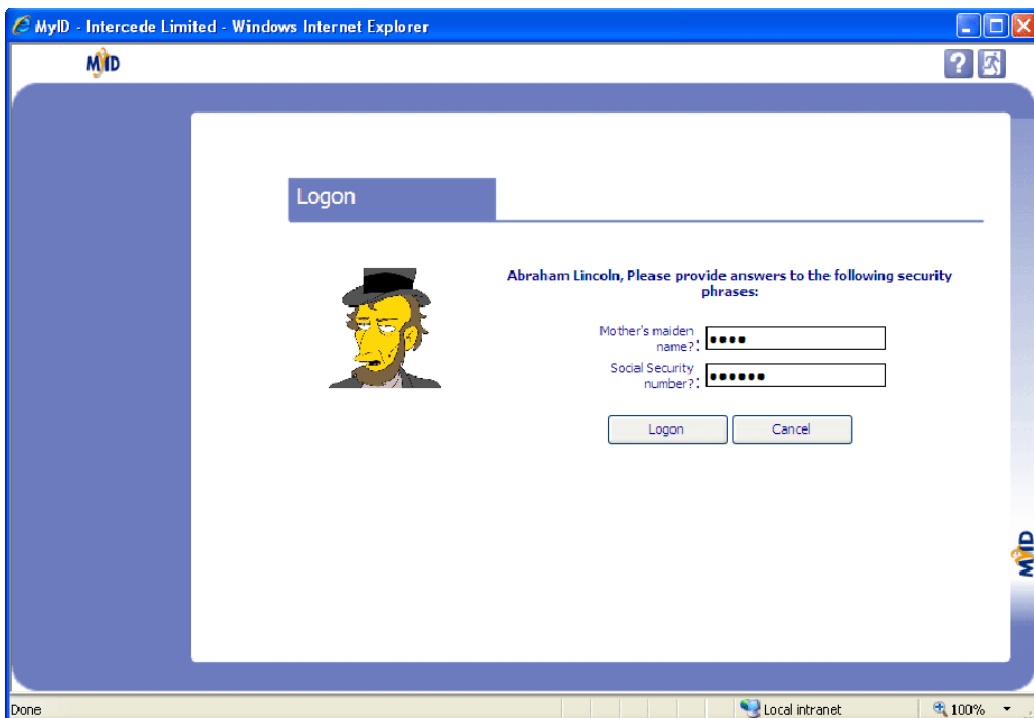
In unserer Beispielinstallation begibt es sich, dass unser Testbenutzer Abraham die PIN seiner Smartcard vergessen hat. Er glaubt, sich erinnern zu können und versucht mehrere male sich mit einer falschen PIN anzumelden und als er das voreingestellte Limit erreicht, ist seine Karte gesperrt.



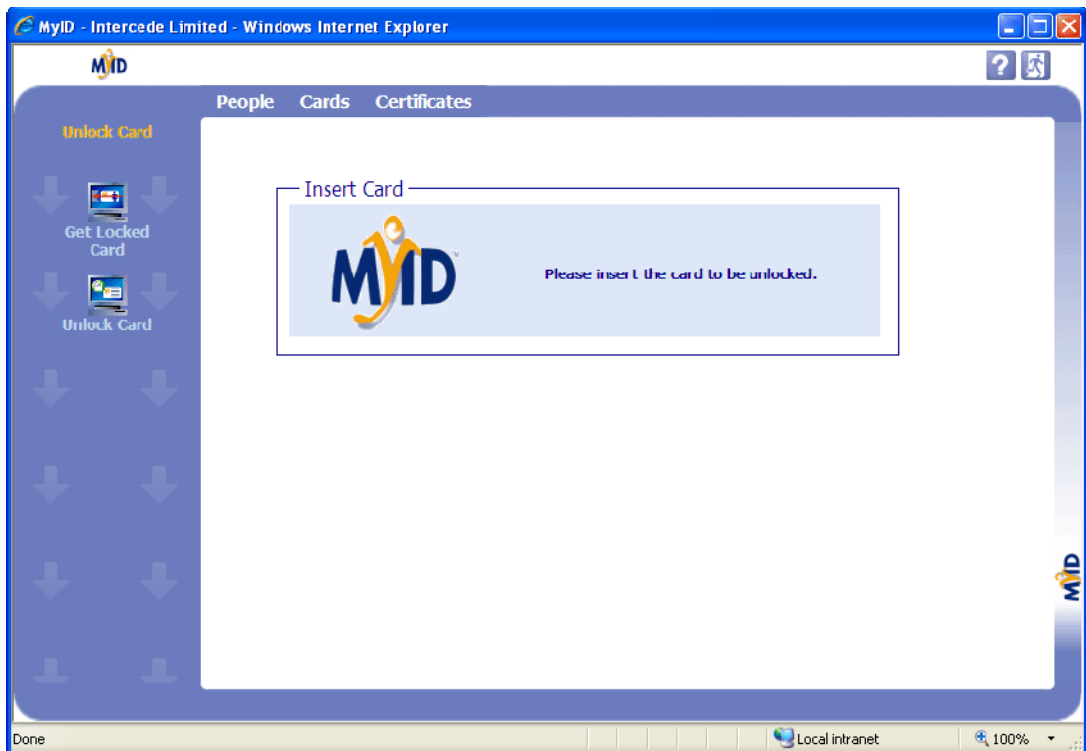
Da kein öffentliches Terminal vorhanden ist, bittet er einen angemeldeten Kollegen, an seinem Computer die Security Management Console zu öffnen, ohne eine Karte in den Smartcard Reader einzulegen. Dort gibt er dann seinen Windows Benutzernamen in das „**User Name**“ Feld ein und klickt auf „**Logon**“.



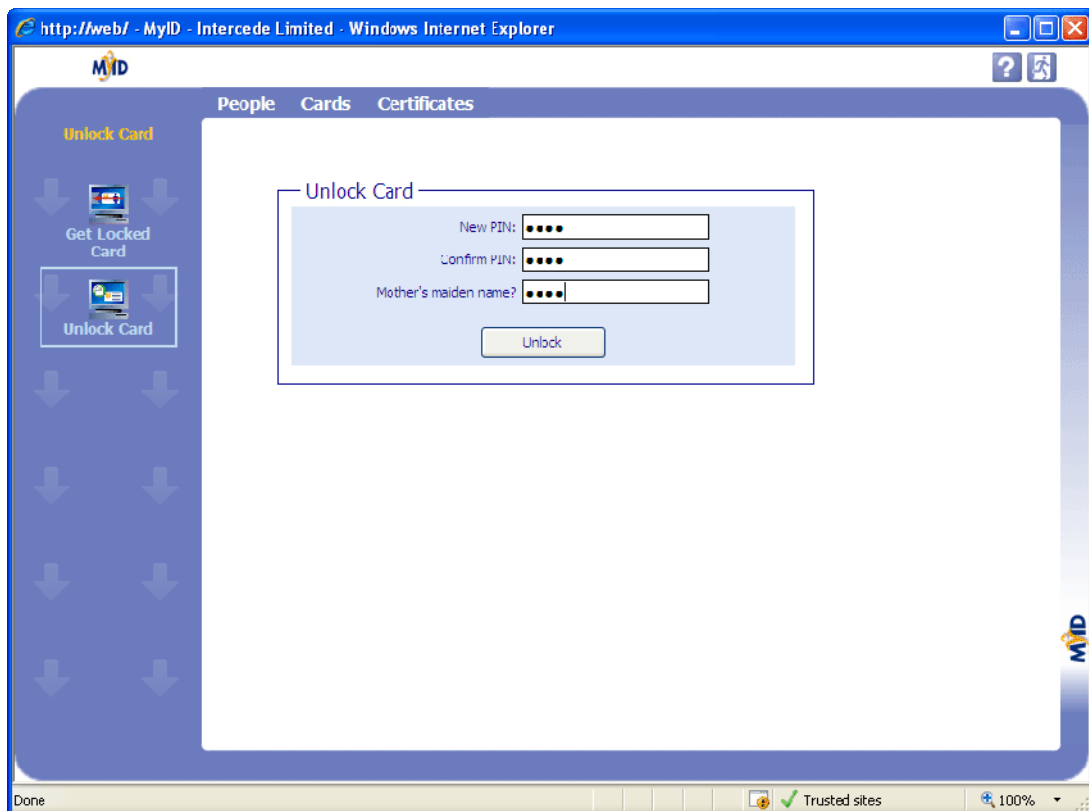
Schon erscheint sein Anmeldefenster, in dem er sich mit den vorbereiteten Antworten authentisieren kann.



Hier kann er nun das Applet „Unlock Card“ im Navigationsbalken (links) aufrufen:



Nachdem er seine Karte eingelegt hat, kann er eine neue PIN wählen....



.... und seine Karte entsperren. Dazu muss er noch einmal eine seiner Authentisierungsfragen beantworten. -> „unlock“

-> Fertig. Er kann sich nun wieder mit seiner eigenen Smartcard anmelden.

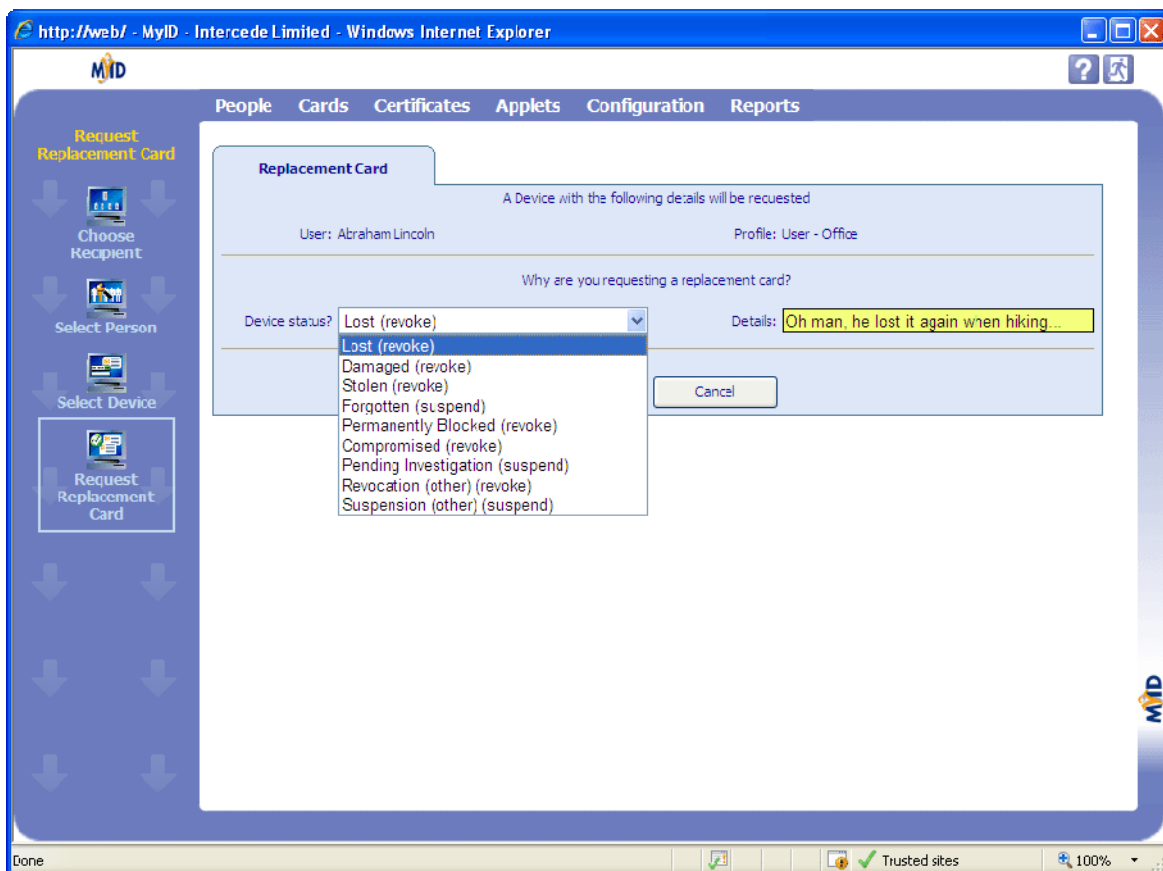
Tipp: Bevor unser Benutzer das Terminal oder den Computer des Kollegen verlässt, klickt er noch einmal auf das „kleine Männchen“ rechts oben in der Konsole um sich von der Konsole abzumelden.

## Ersatz einer verlorenen Smartcard

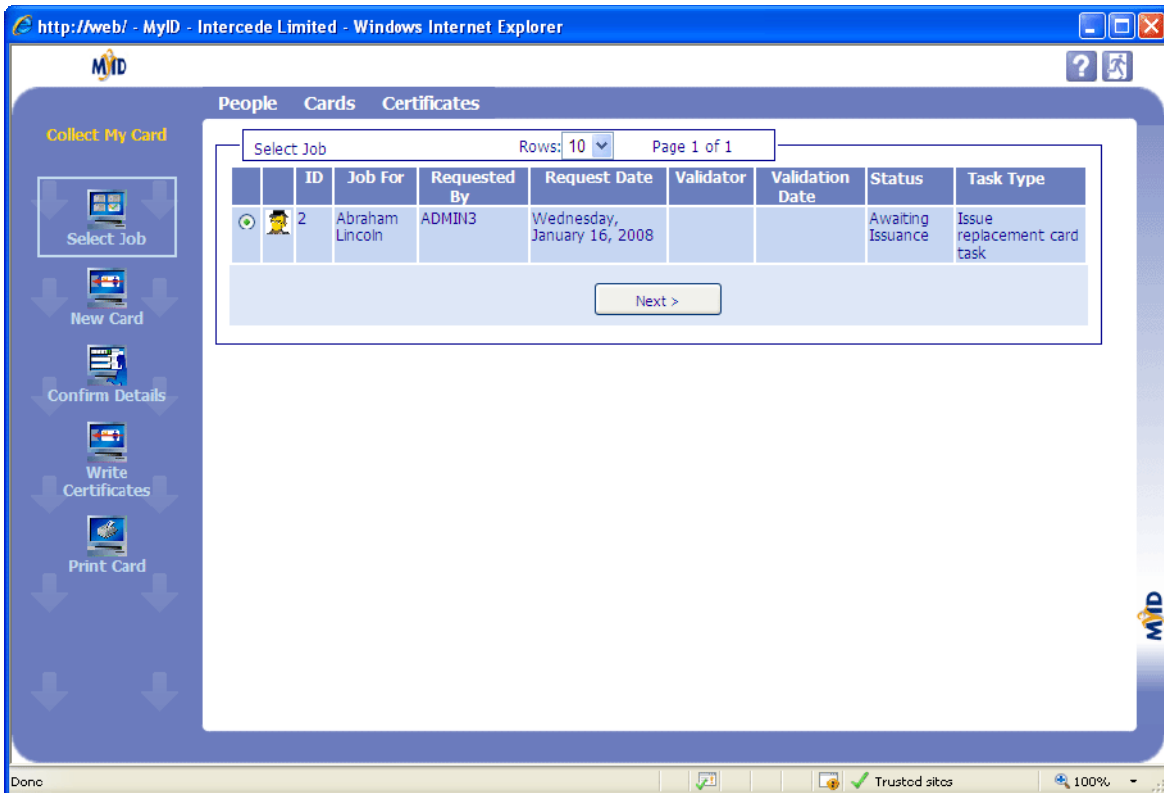
Wenn ein Benutzer seine Smartcard verloren oder vergessen hat, oder den Verdacht hat, sie wurde kopiert oder manipuliert, so kann er in der Security Management Console (sofern das System dazu eingerichtet wurde) eine Ersatzkarte erstellen.

Nehmen wir an, unser Testbenutzer Abraham hat seine Smartcard verloren. Er ruft beim Helpdesk (in unserem Falle beim Administrator des Testlabors) an und erklärt sein Missgeschick.

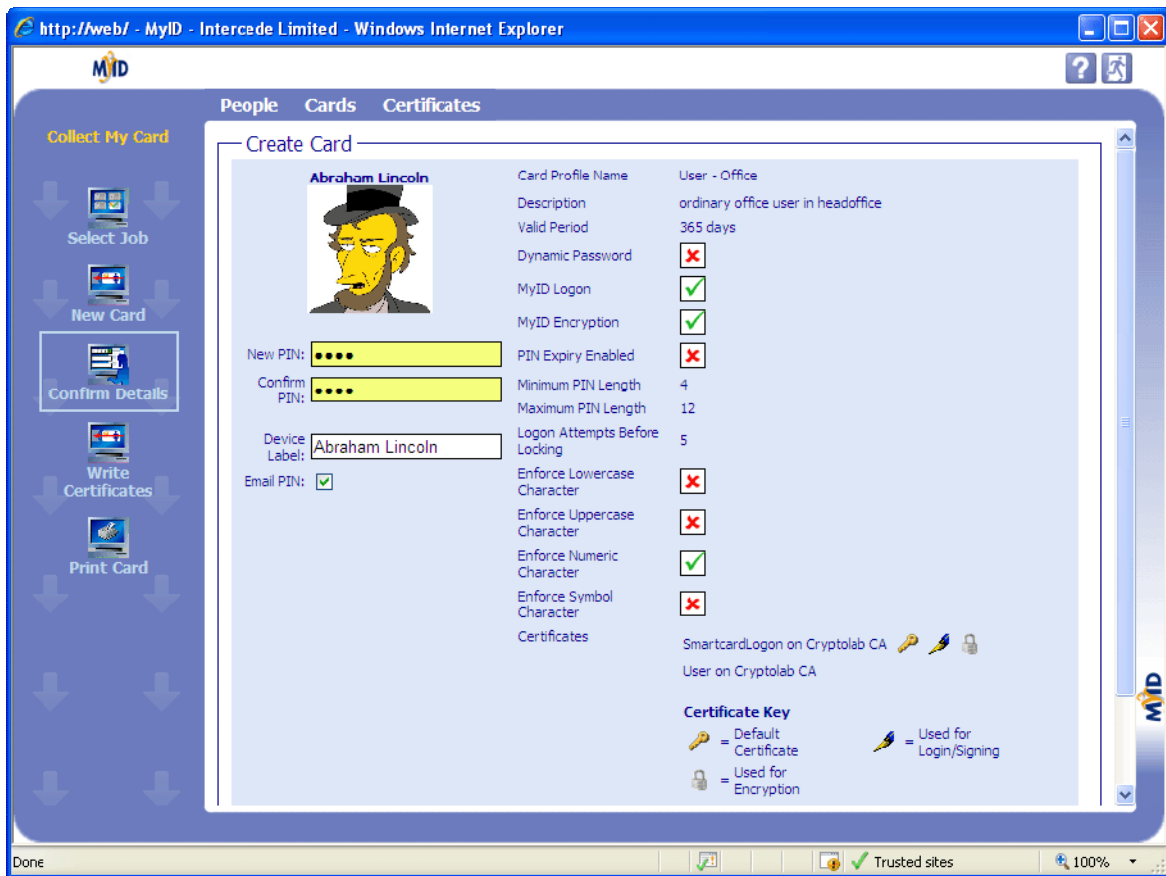
Dieser startet das Applet „Request Replacement Card“ und wählt den betroffenen Benutzer aus.



Unser Testbenutzer besorgt sich nun eine neue Smartcard (bei der Personalabteilung oder dem IT Helpdesk etwa) und begibt sich wieder zu einem Terminal oder zu einem hilfsbereiten Kollegen . Dort meldet sich an der Konsole mit der alternativen Anmeldung, also mit den Authentisierungsfragen an. Dann startet er das Applet „Collect my Card“



Er legt seine neue Karte in das Lesegerät und klickt auf „Next“



Nun gibt er eine PIN ein, die den Richtlinien der Organisation entsprechen und klickt auf  
-> „Next“

Fertig, er hat eine neue Karte

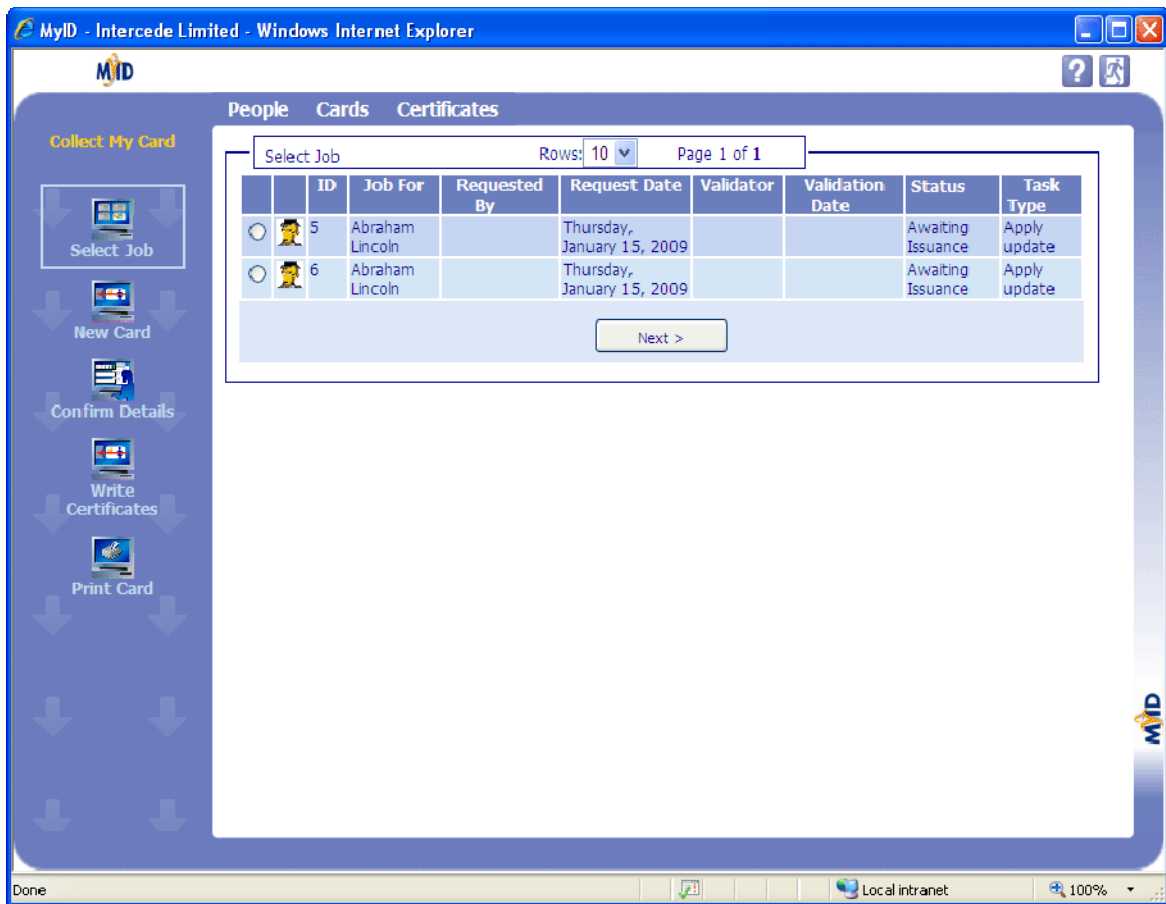
Tipp: Wenn wir den Benutzern erlauben wollen, die Ersatzkarten selbst auszustellen, so sollten wir entweder bereits vorgedruckte, leere Karten vorbereiten oder ein Terminal mit Kartendrucker zur Verfügung stellen. Wenn wir den Benutzern nicht zutrauen, mit „Skip Printing“ den Kartendruck abzubrechen (kein Kartendrucker verfügbar), wählen wir für die Ersatzkarten ein Profil ohne Layout.

## Erneuern der ablaufenden Zertifikate auf der Smartcard

Wenn ein oder mehrere Zertifikate auf der Smartcard des Benutzers ablaufen, erhält er rechtzeitig von MyID eine Email mit einer Verständigung darüber.

Tip: Der Inhalt und das Aussehen der Email kann vom Administrator frei gestaltet werden. Sie sollte aber außer dem Hinweis auf die Erneuerung auch eine kleine Anweisung, wie denn nun vorzugehen ist und vielleicht auch die Telefonnummer eines Helferleins beinhalten. Außerdem denken wir dabei auch wieder an die CI der Organisation.

Nun meldet sich unser Testbenutzer wieder mit seiner noch funktionierenden Smartcard am der Security Management Console von MyID an und startet das Applet „Collect my Card“



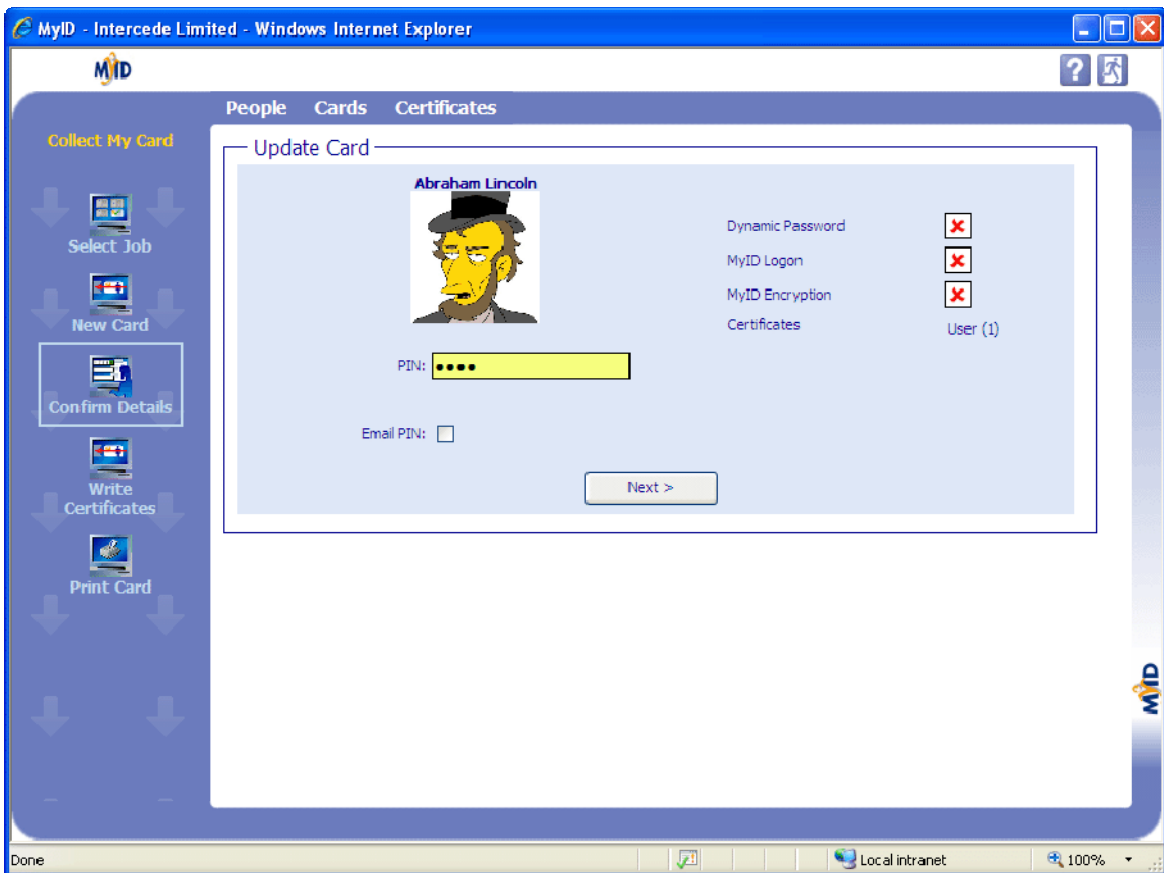
The screenshot shows the MyID web application interface in a Windows Internet Explorer browser window. The page title is "MyID - Intercede Limited - Windows Internet Explorer". The interface has a blue header with the MyID logo and navigation tabs for "People", "Cards", and "Certificates". On the left side, there is a vertical menu with icons and labels for "Collect My Card", "Select Job", "New Card", "Confirm Details", "Write Certificates", and "Print Card". The main content area displays a table of certificates with the following data:

ID	Job For	Requested By	Request Date	Validator	Validation Date	Status	Task Type
5	Abraham Lincoln		Thursday, January 15, 2009			Awaiting Issuance	Apply update
6	Abraham Lincoln		Thursday, January 15, 2009			Awaiting Issuance	Apply update

Below the table is a "Next >" button. The browser's status bar at the bottom shows "Done", "Local intranet", and "100%".

Unser Testbenutzer hat 2 Zertifikate auf seiner Smartcard, die beide bald ablaufen werden und daher vom System automatisch zur Erneuerung beantragt wurden

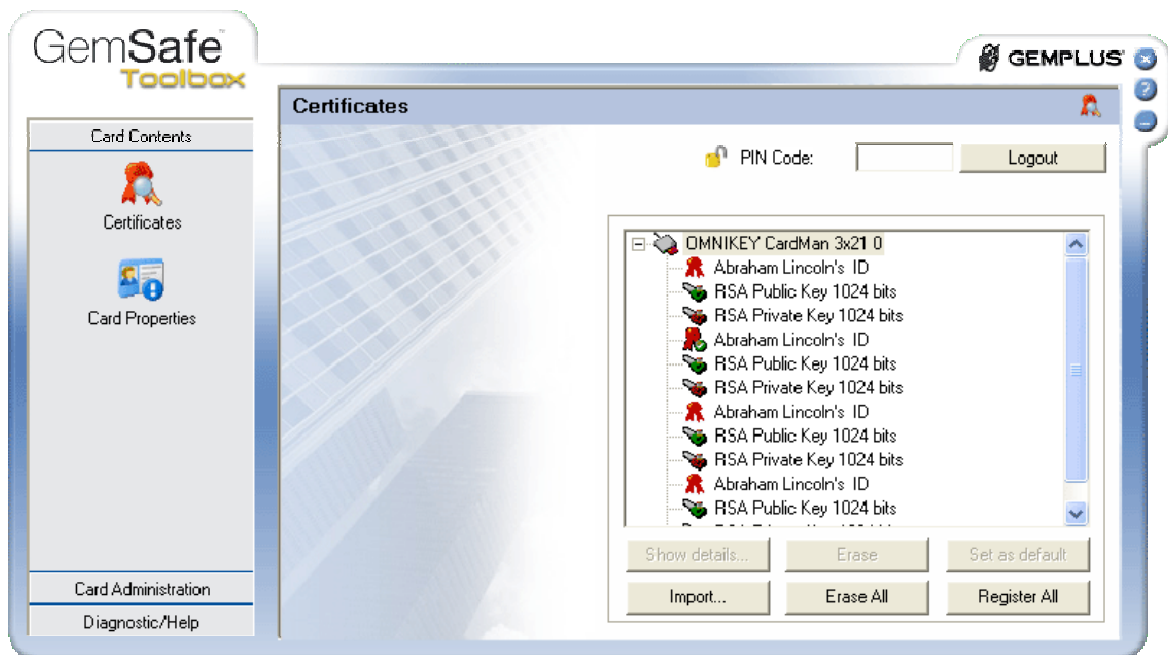
Er wählt also eine dieser Aufgaben an und klickt auf „Next“



Er gibt seine PIN an, klickt auf Next, und „Skip Printing“ (er möchte ja seine alte Karte mit neuen Zertifikaten weiterverwenden) und wiederholt diesen Vorgang für alle Zertifikate, die auf seiner Karte erneuert werden müssen.... Also insgesamt 2 mal in unserem Falle.

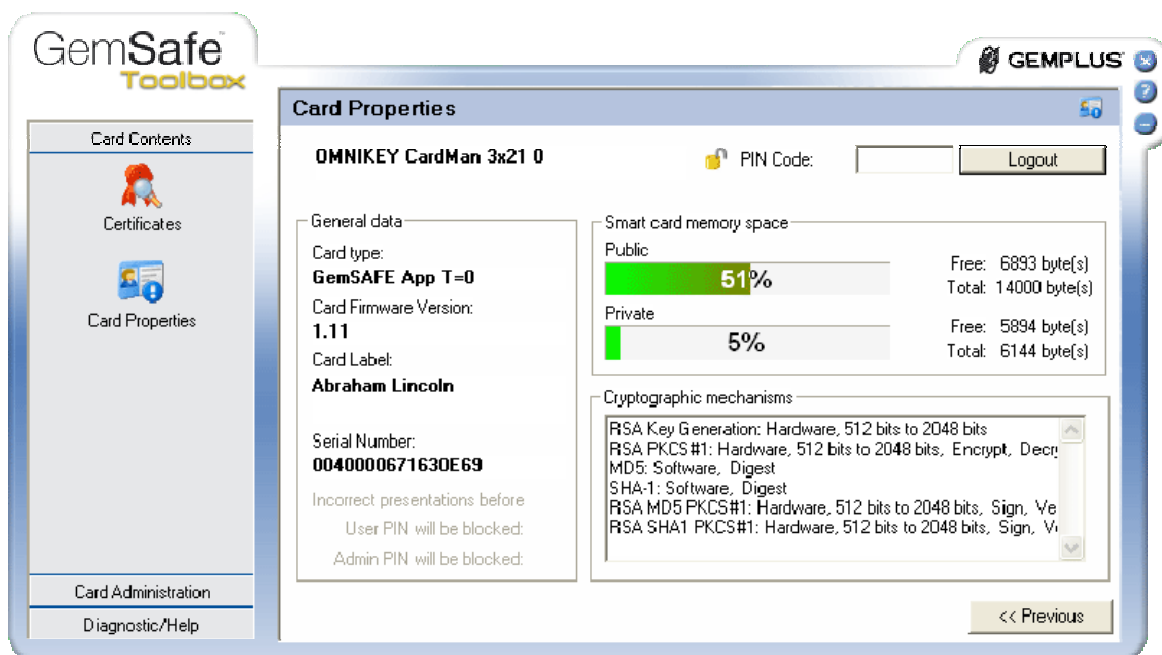
Fertig.

Ein Blick auf den Inhalt unserer Smartcard zeigt uns, dass in unserem Falle zusätzlich zu den alten Zertifikaten, neue ausgestellt und auf die Karte geschrieben wurden.



Tipp: Dieses Verhalten (neues Zertifikat mit neuem Schlüssel) ist abhängig von den Einstellungen in Intercede MyID. Wenn die privaten Schlüssel der Benutzer nicht archiviert wurden, müssen bei Ablauf der alten Zertifikate selbstverständlich neue Schlüsselpaare erstellt werden.

Und noch etwas, das unbedingt bei der Planung des Smartcard Einsatzes im Unternehmen berücksichtigt werden sollte (ein Konzept.... nirgends ist es so wichtig ein Konzept zu erstellen, als in der Planung der IT Sicherheitsmaßnahmen!)



Smartcards haben nur einen begrenzten Speicherplatz, der von Karte zu Karte variiert. Daher sollten geplante Lebensdauer der Smartcards, Größe der Zertifikate (Schlüssellänge), Anzahl der verwendeten Zertifikate und deren Zweck und Lebensdauer sowie das Verhalten bei Erneuerung unbedingt bei der Erstellung des Konzeptes berücksichtigt werden. Und dieses Konzept sollte unbedingt bestehen, bevor wir uns zum Kauf einer Smartcard und für eine Sicherheitsarchitektur entschieden haben.

CRYPTAS it-Security  
Modcenterstrasse 22/B2  
A-1030 Wien, Austria  
T +43 (1) 798 96 96 – 0  
F +43 (1) 798 96 96 – 99  
info@cryptas.com

[www.cryptoshop.com](http://www.cryptoshop.com)  
[www.cryptas.com](http://www.cryptas.com)