SafeNet Authentication Client

Integration Guide

Using SAC CBA for IBM Notes

Document Information

Document Part Number	007-012954-001, Rev. A
Release Date	April 2015

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as IBM Notes.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

This document describes how to enable smart card logon options in IBM Notes using SafeNet USB Tokens managed by SafeNet Authentication Client.

SafeNet Authentication Client (SAC) is a public key infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. SafeNet's certificate-based tokens provide secure remote access, as well as other advanced functions, in a single token, including digital signing, password management, network logon, and combined physical/logical access.

The tokens come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are interfaced using a single middleware client, SafeNet Authentication Client (SAC). The SAC generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications, offering secure web access, secure network logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

SafeNet Authentication Manager (SAM) provides your organization with a comprehensive platform to manage all of your authentication requirements, across the enterprise and the cloud, in a single, integrated system. SAM enables management of the complete user authentication life cycle. SAM links tokens with users, organizational rules, and security applications to allow streamlined handling of your organization's authentication infrastructure with a flexible, extensible, and scalable management platform.

SAM is a comprehensive token management system. It is an out-of-the-box solution for Public Certificate Authorities (CA) and enterprises to ease the administration of SafeNet's hardware or software tokens devices. SAM is designed and developed based on the best practices of managing PKI devices in common PKI implementations. It offers robust yet easy to customize frameworks that meets different organizations' PKI devices management workflows and policies. Using SAM to manage tokens is not mandatory, but it is recommended for enterprise organizations.

For more information, refer to the *SafeNet Authentication Manager Administrator Guide*.

IBM Notes software client is a single point of access that simplifies the integration of messaging, business applications, and social collaboration into one easy-to-use workspace.

Without the use of a smart card, you only need your User ID and IBM Notes password to access the application. The advantage of using a smart card is that you can lock your User ID, which adds another layer of protection. Using a smart card, you need your User ID, smart card, and smart card PIN to access the application. And because you carry your smart card with you (just as you would carry a credit card), you are much less vulnerable to User ID theft.

It is assumed that the IBM Notes environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

Applicability

The information in this document applies to:

- **SafeNet Authentication Client (SAC)** — SafeNet Authentication Client is the middleware that manages SafeNet's tokens.
- **IBM Notes Social Edition**

Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Client (SAC)** —Version 9.0
- **IBM Notes Social Edition** —Version 9.0

Audience

This document is targeted to system administrators who are familiar with IBM Notes and are interested in adding smart card logon capabilities in IBM Notes using SafeNet tokens.

Authentication Flow using SAC

The diagram below illustrates the flow of smart card logon for IBM Notes using the SafeNet smart card or eToken.

1. A user attempts to connect to the IBM Notes server using the IBM Notes client application.
2. The user inserts the SafeNet token on which his certificate resides, and, when prompted, enters the token password.

3. After successful authentication, the user is allowed access to IBM Notes.

Prerequisites

This section describes the prerequisites that must be installed and configured before implementing smart card logon for IBM Notes using SafeNet tokens:

- SafeNet Authentication Client (v9.0) should be installed on all client machines.
- A pre-loaded Internet certificate and key is present on the SafeNet smart card or eToken.
- IBM Notes should be installed and configured with domino server.
- If SAM is used to manage the tokens, TPO should be configured with MS CA Connector. For further details, refer to the section “Connector for Microsoft CA” in the *SafeNet Authentication Manager Administrator’s Guide*.
- Users must have a SafeNet token with an appropriate certificate enrolled on it.

Supported Tokens in SAC

SAC supports a number of tokens that can be used as second authentication factor for users who authenticate to IBM Notes.

SafeNet Authentication Client 9.0 (GA) supports the following tokens:

Certificate-based USB tokens

- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID and VSR

Smart Cards

- SafeNet eToken PRO Smartcard 72K
- SafeNet eToken 4100

Certificate-based Hybrid USB Tokens

- SafeNet eToken 7300
- SafeNet eToken 7300-HID
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)

Software Tokens

- SafeNet eToken Virtual
- SafeNet eToken Rescue

Configuring IBM Notes

This section covers two ways to enable smart card login in IBM Notes, and, for an additional layer of protection, how to store Internet private keys on a smart card.

NOTE: This method assumes that the Internet certificate that you will use to secure the ID file is stored on the Smartcard. If it is stored in the ID file instead, before performing this procedure you must a) enable Smartcard login by securing the ID file with a secret, and b) move the Internet keys to the Smartcard.

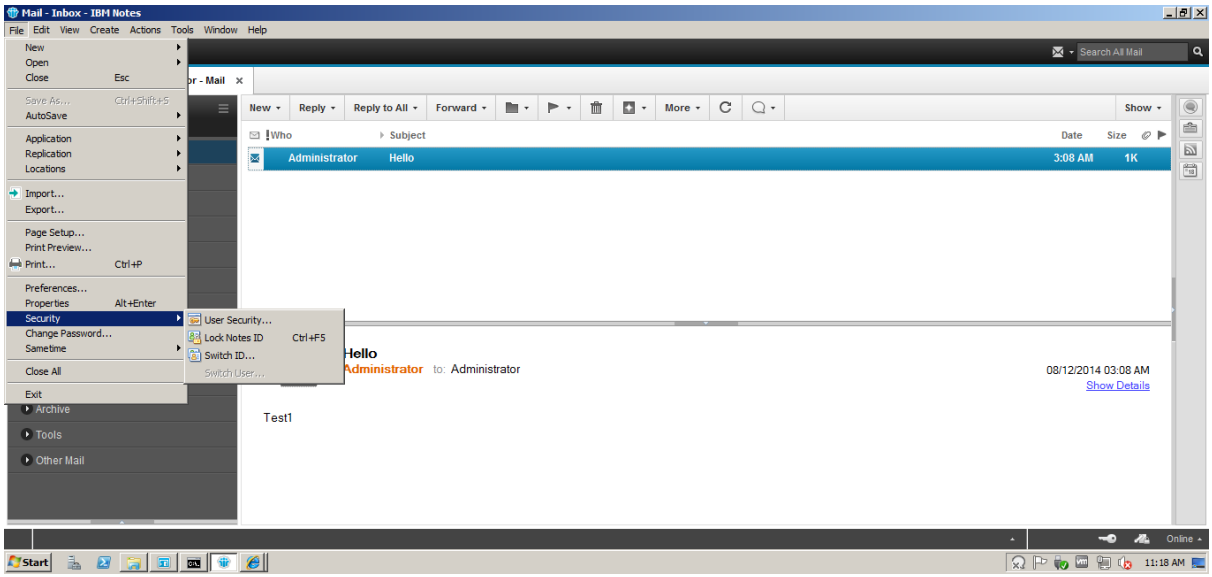
Enabling Smart Card Login to Secure the ID File with an Internet Certificate Key

This type of configuration secures the ID file using a private key from a personal Internet certificate stored on the smart card. This method supports the use of smart cards on which the Internet certificate and keys are pre-loaded, which means there is no need to make changes to the smart card (therefore, read-only smart cards can be used).

NOTE: Once smart card login is enabled for your Notes User ID, you cannot disable it. You will be prompted for your smart card Personal Identification Number (PIN) in place of your IBM Notes password. Please ensure your User ID is recoverable.

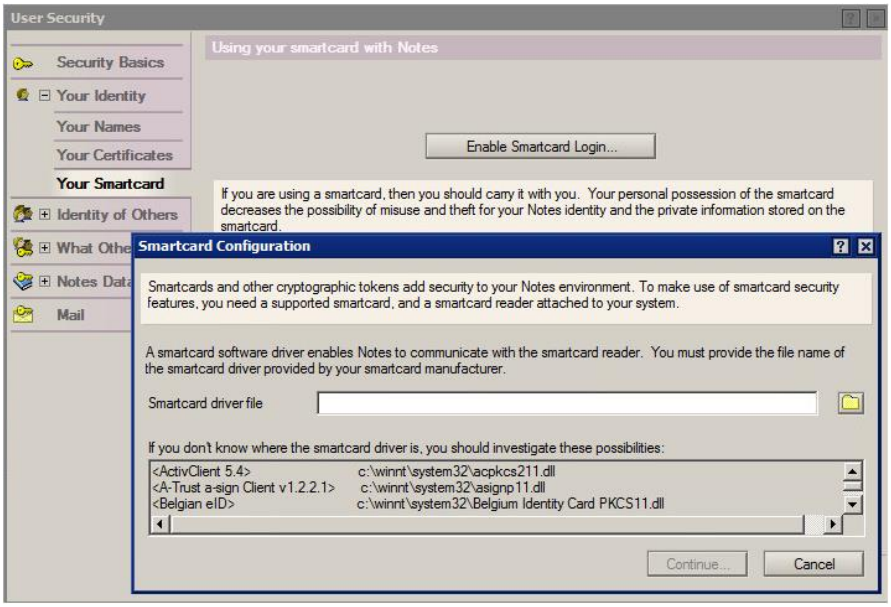
1. On the Windows desktop, double-click **IBM Notes**.

2. On the **IBM Notes** window, select **File** > **Security > User Security**.



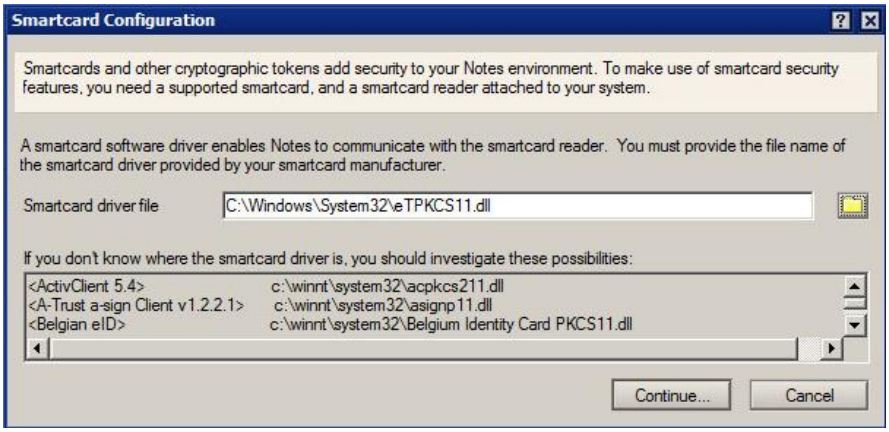
(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

3. On the **User Security** window, select **Your Identity** > **Your Smartcard**.



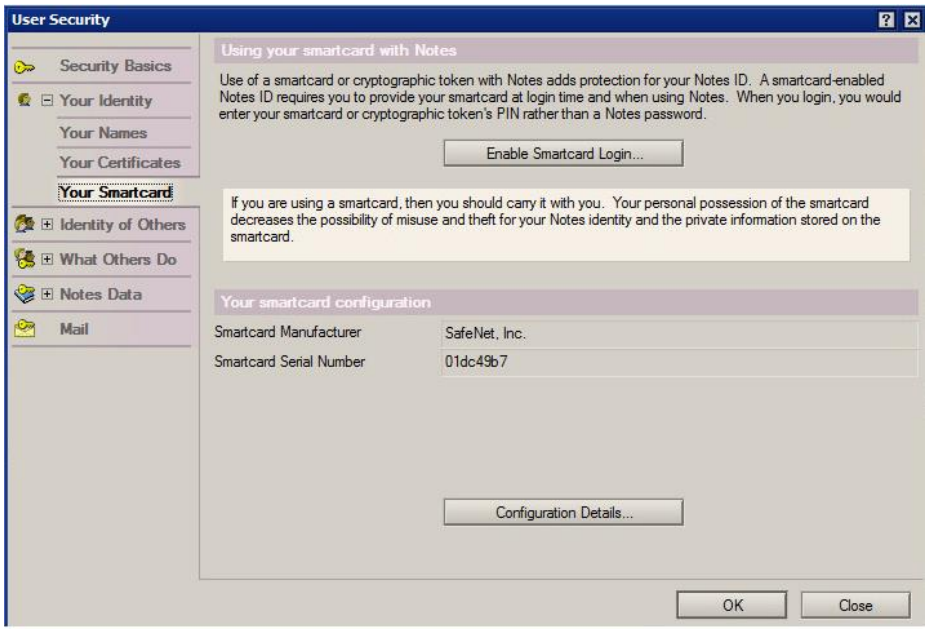
(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

4. On the **Smartcard Configuration** window, click the **Smartcard driver file** folder icon  , browse to the **C:\Windows\System32\eTpkcs11.dll** file, and then click **Continue**.



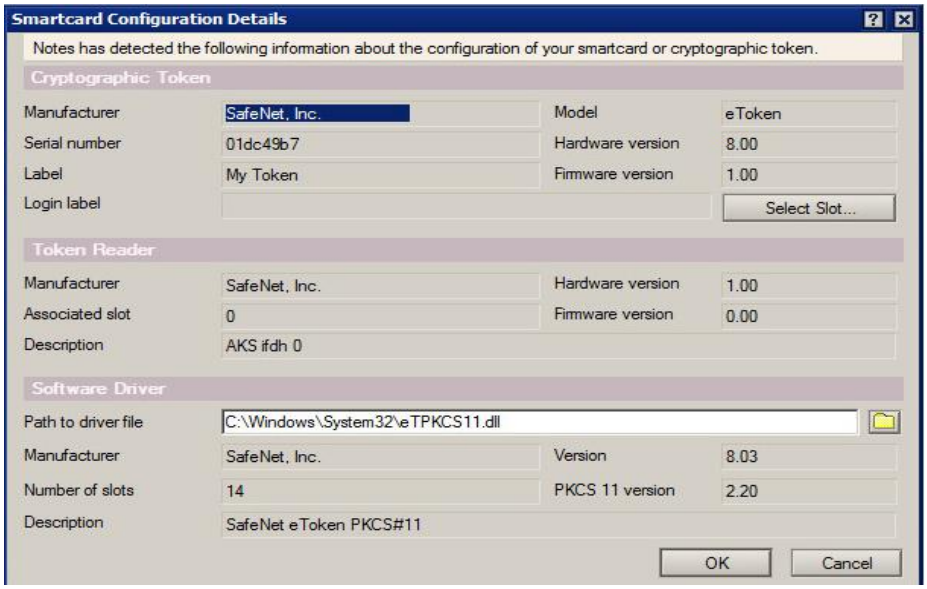
(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

5. Under **Your smartcard configuration**, verify that values are displayed in the **Smartcard Manufacturer** and **Smartcard Serial Number** fields.



(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

6. Click **Configuration Details**.
7. Review the smartcard configuration information, and then click **OK**.



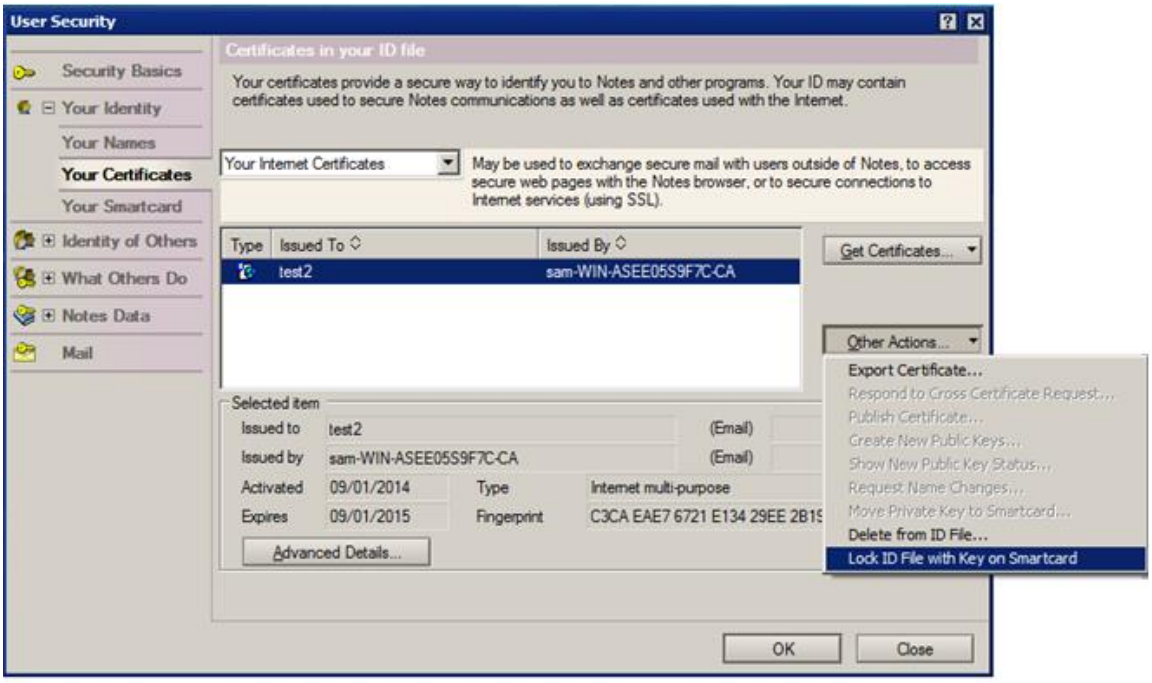
(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

8. Select **Your Identity > Your Certificates**. Complete the following steps, and then click **OK**.

   a. Click the **Your Internet Certificates** menu, and then select the certificate to use to secure the ID file.

> **NOTE:** To import Internet certificates from smart card and store them in the Lotus Notes ID file, refer Appendix.

   b. Click the **Other Actions** menu, and then select **Lock ID File with Key on Smartcard**.

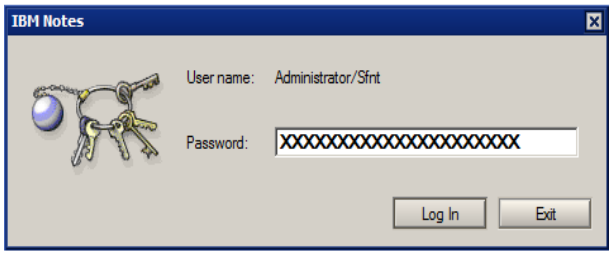


(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

9. When this warning message is displayed, click **OK**.

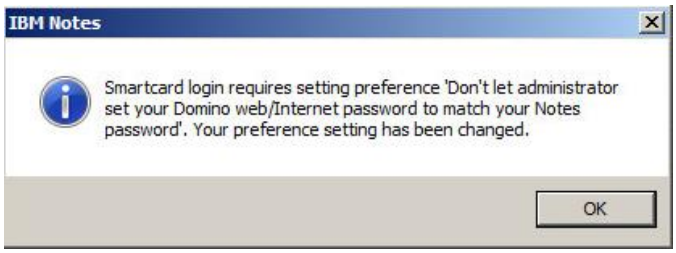
(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

10. When this window is displayed, enter the user account **Password**, and then click **Log In**.

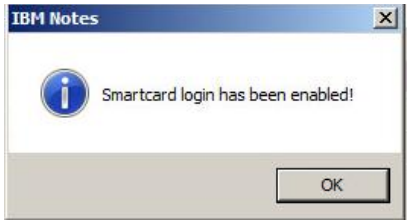


(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

11. When the following messages are displayed, click **OK**.

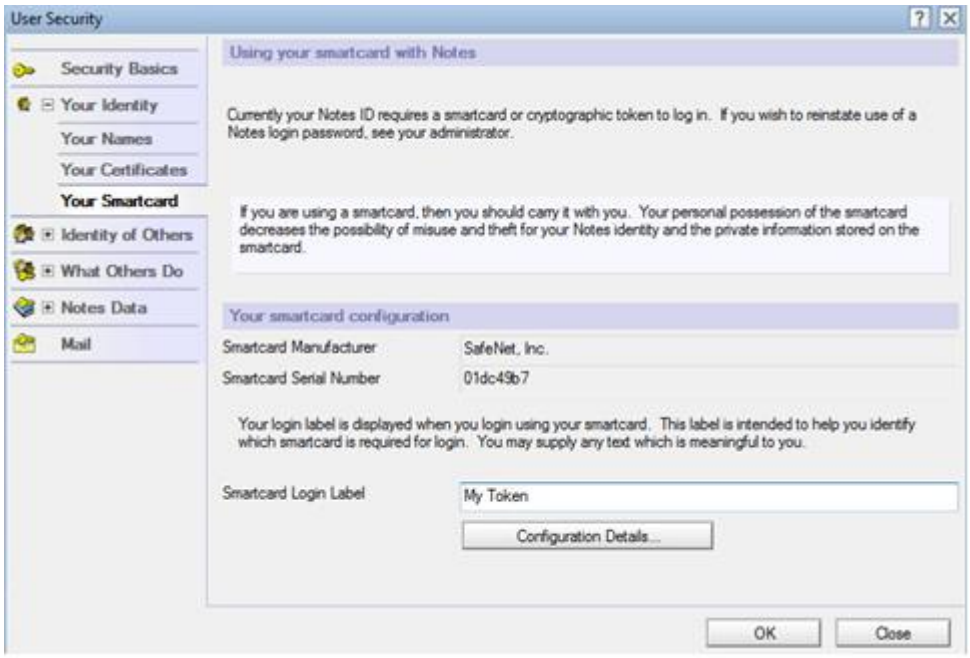


(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).



(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

12. On the **User Security** window, click **OK** to save the changes.
13. Select **Your Identity > Your Smartcard**.
14. In the **Smartcard Login Label** field, enter a descriptive name to identify the smart card (for example, **My Token**), and then click **OK**.



(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

15. When this message is displayed, click **OK**.

(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

16. Close IBM Notes.

Now, every time you log in to IBM Notes, you will need to use your smart card PIN.

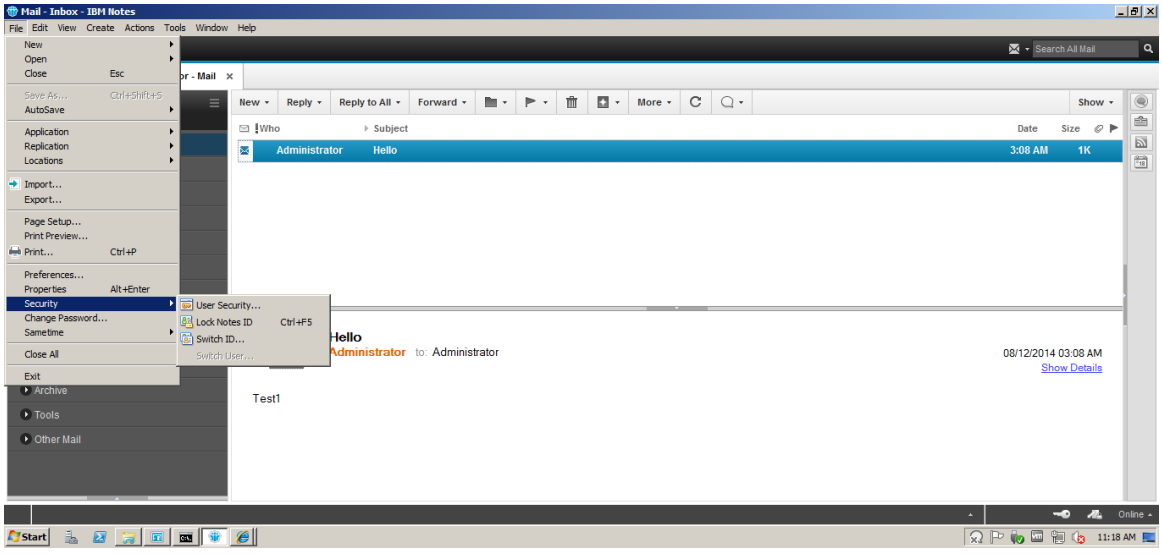
Enabling Smart Card Login to Secure the ID File with a Secret Stored on the Smart Card

This type of configuration secures the ID file using a secret that is added to the smart card.

NOTE: Once smart card login is enabled for your IBM Notes User ID, you cannot disable it. You will be prompted for your smart card Personal Identification Number (PIN) in place of your IBM Notes password. Please ensure your User ID is recoverable.

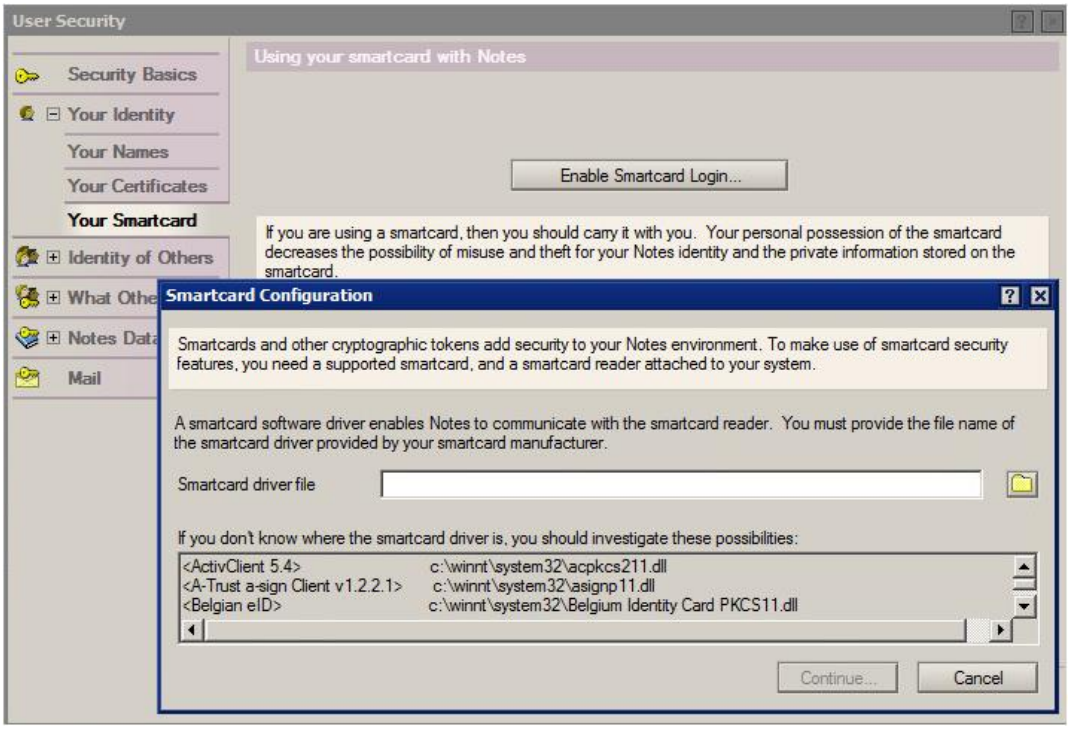
1. On the Windows desktop, double-click **IBM Notes**.

2. On the **IBM Notes** window, select **File** > **Security > User Security**.

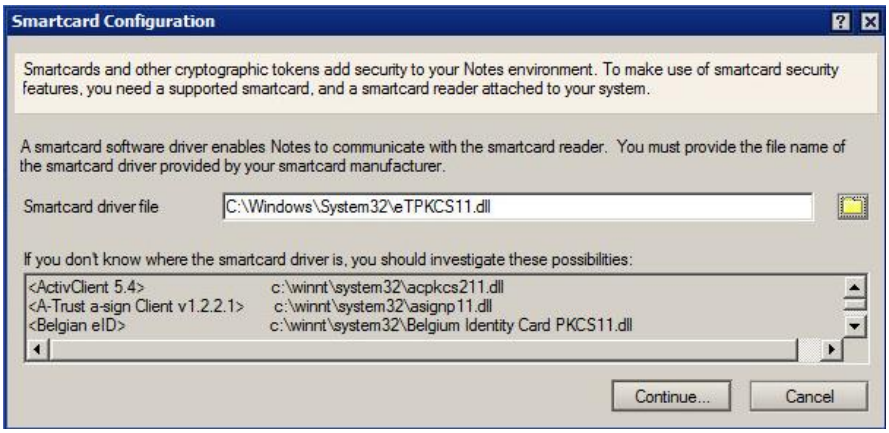


(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

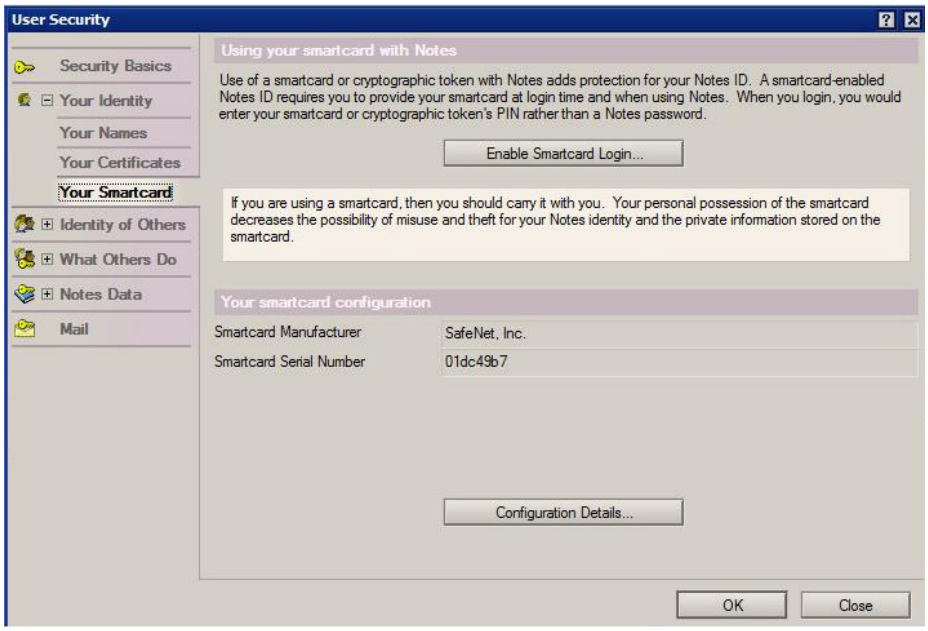
3. On the **User Security** window, select **Your Identity** > **Your Smartcard**.



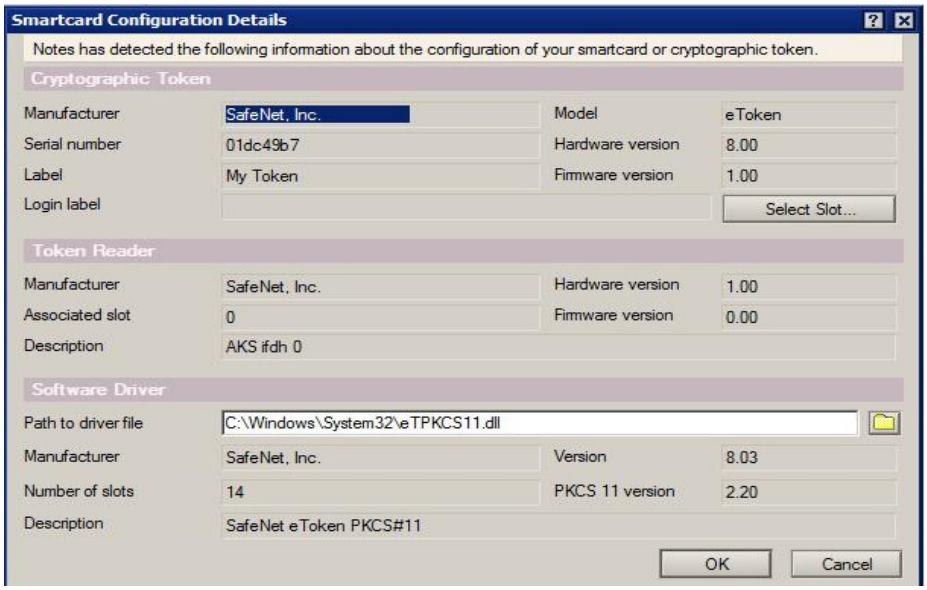
4. On the **Smartcard Configuration** window, click the **Smartcard driver file** folder icon  , browse to the **C:\Windows\System32\eTpkcs11.dll** file, and then click **Continue**.



5. Under **Your smartcard configuration**, verify that values display in the **Smartcard Manufacturer** and **Smartcard Serial Number** fields.



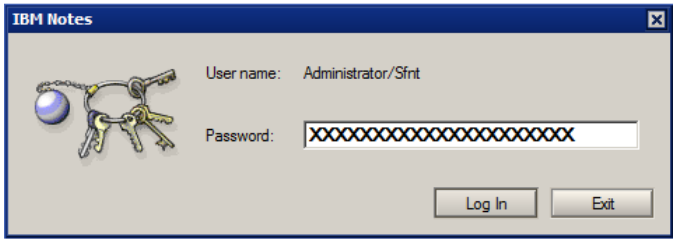
6. Click **Configuration Details**.
7. Review the smartcard configuration information, and then click **OK**.



8. Under **Using your smartcard with Notes**, click **Enable Smartcard Login**.
9. When this warning message is displayed, click **OK**.

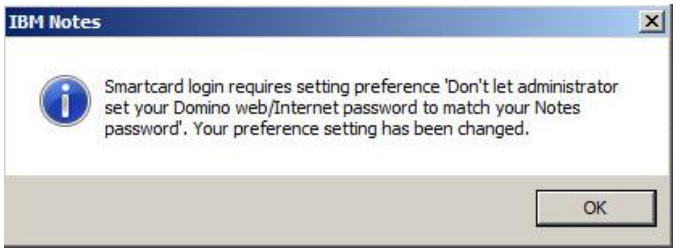
(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

10. When this window is displayed, enter the user account **Password**, and then click **Log In**.

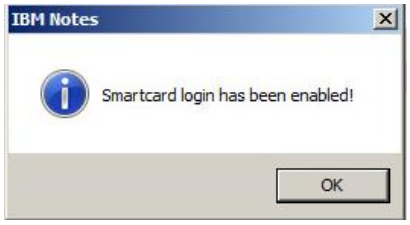


(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

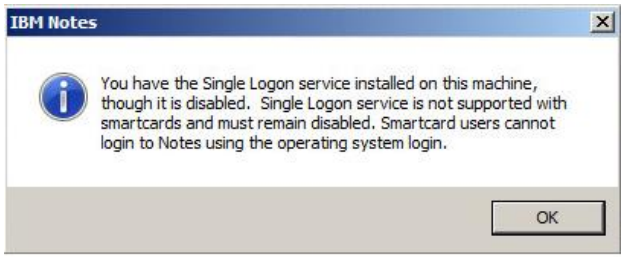
11. When the following messages are displayed, click **OK**.



(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

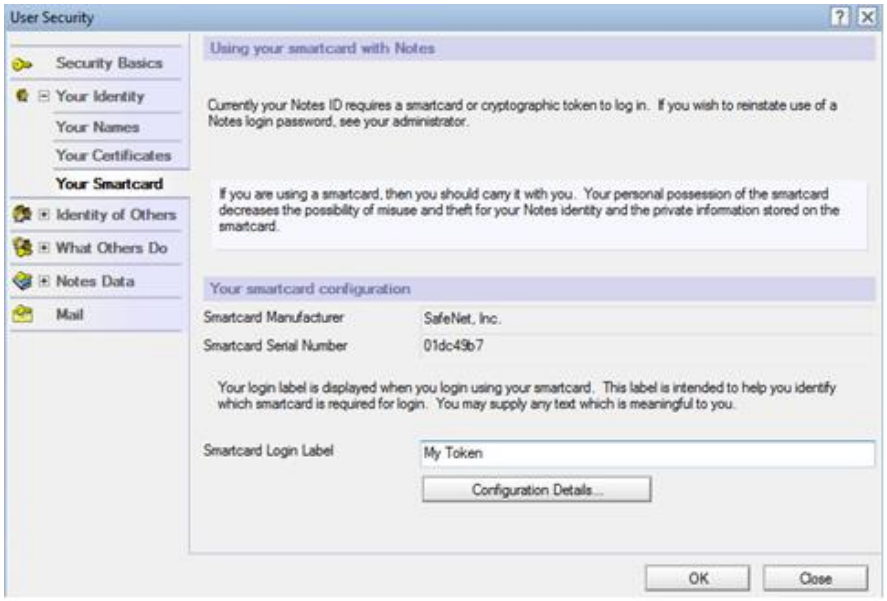


(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).



(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

12. On the **User Security** window, click **OK** to save the changes.
13. Select **Your Identity > Your Smartcard**.
14. In the **Smartcard Login Label** field, enter a descriptive name to identify the smart card (for example, **My Token**), and then click **OK**.



(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

15. When this message is displayed, click **OK**.

(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

16. Close IBM Notes.

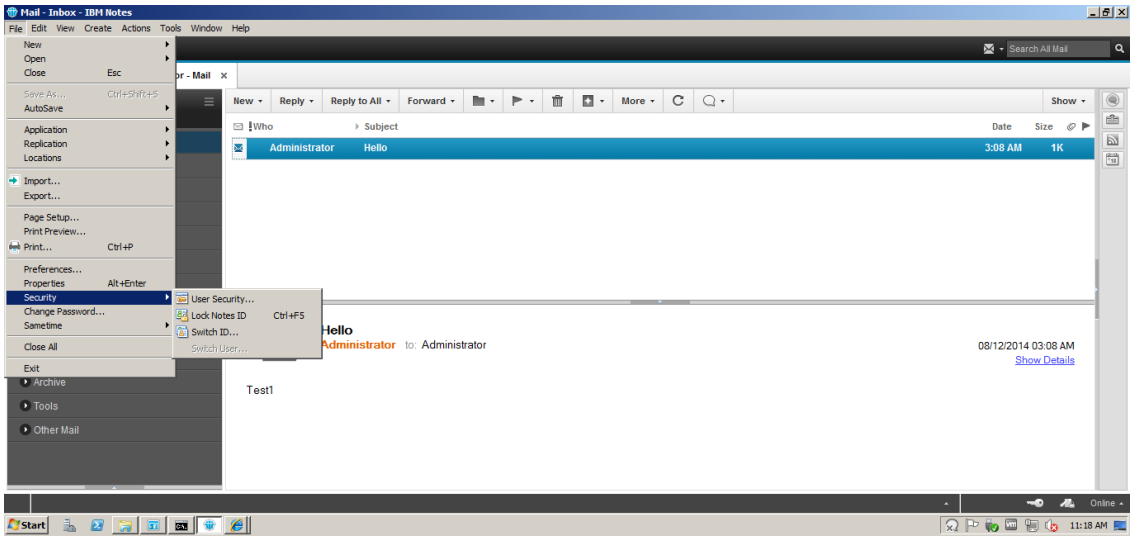
Storing Internet Private Keys on a Smart Card

Any Internet private keys that you have from personal Internet certificates (not from Internet certificate authority certificates) can be stored on your smart card.

Storing Internet private keys on your smart card adds an extra level of protection for them, rather than just storing them in your User ID. Once a private key is moved to a smart card, it is only possible to export the certificate (without including the private key) to a separate file.

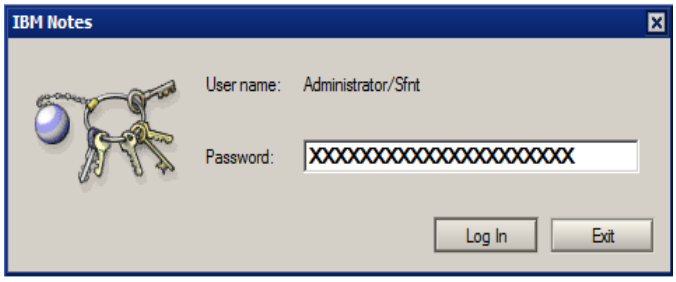
1. On the Windows desktop, double-click **IBM Notes**.

2. On the **IBM Notes** window, select **File** > **Security > User Security**.



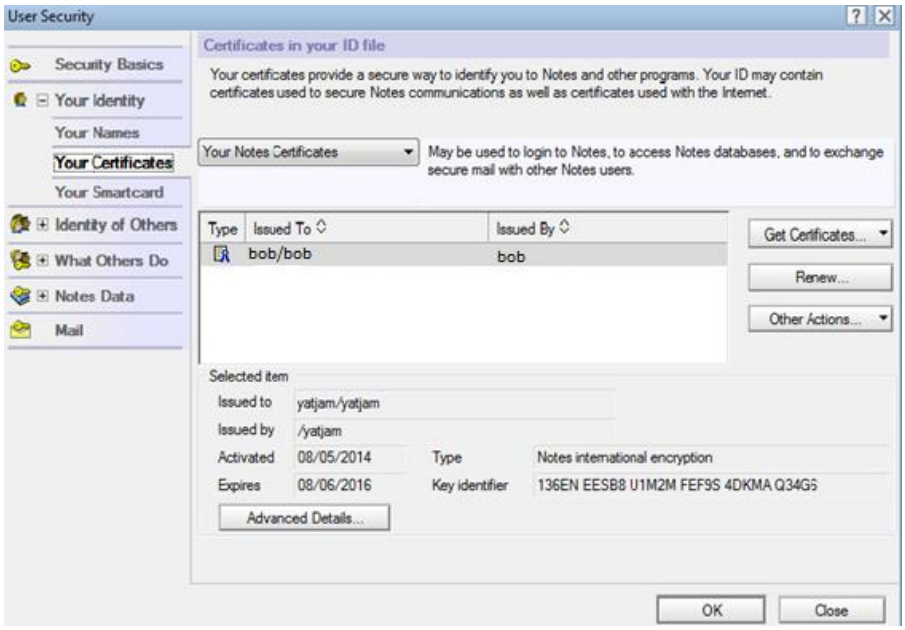
(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

3. When this window is displayed, enter the user account **Password**, and then click **Log In**.



(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

4. On the **User Security** window, select **Your Identity > Your Certificates**.

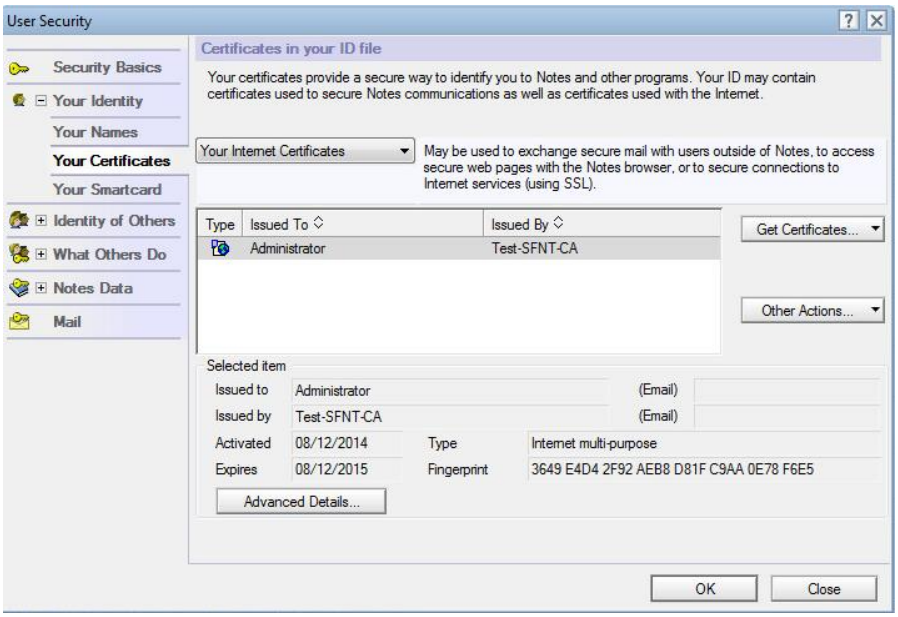


(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

5. If you already have an Internet certificate installed in IBM Notes, click the **Your Internet Certificates** menu, select the certificate to move to your smart card, and then proceed to step 6.

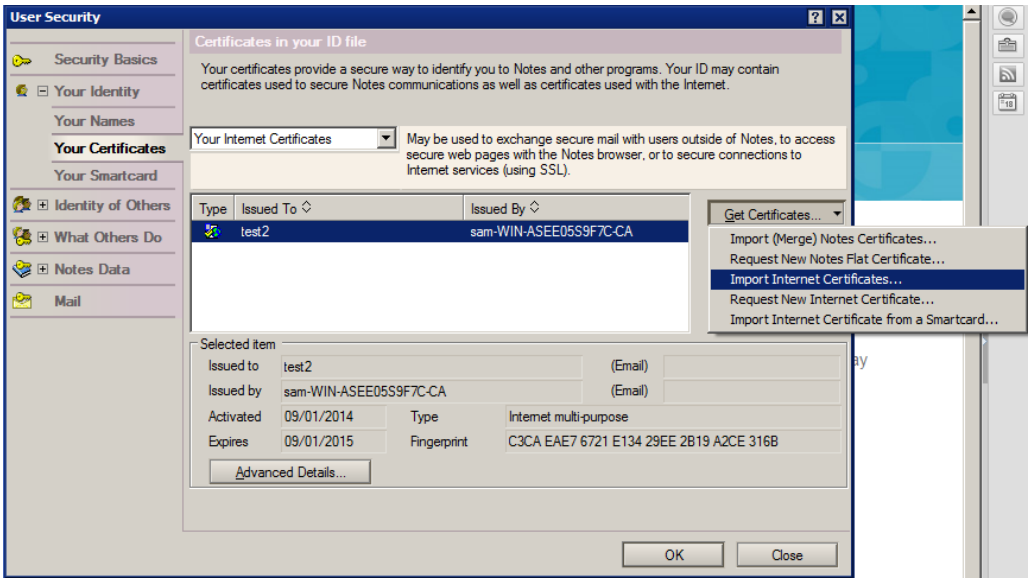
   If you do **not** have an Internet certificate installed in IBM Notes, follow the steps below to import an Internet certificate into the IBM Notes ID file, and then proceed to step 6.

   a. Click the **Your Internet Certificates** menu.



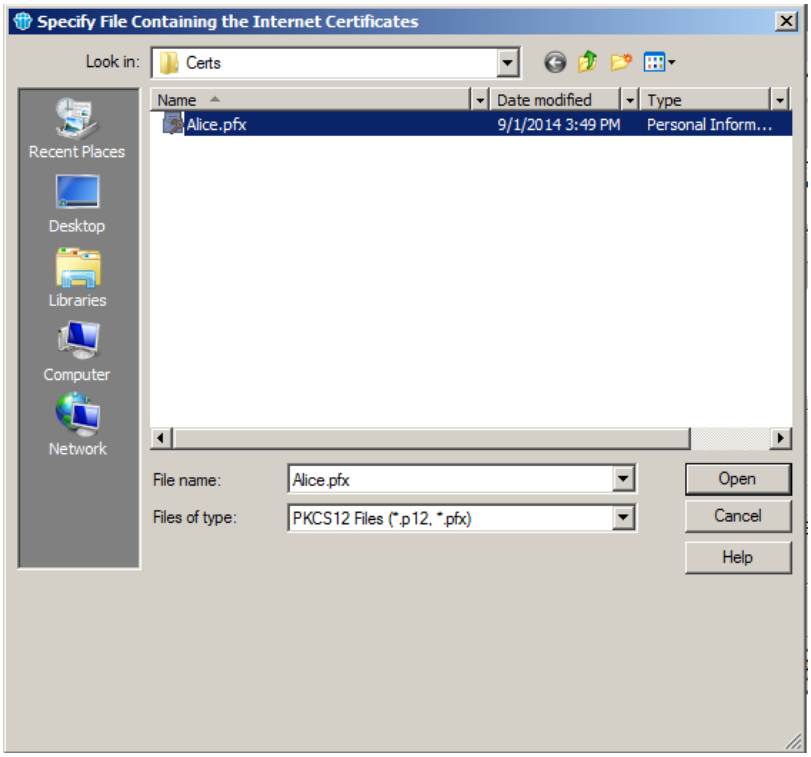
(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

b. Click **Get Certificates**, and then select **Import Internet Certificates**.



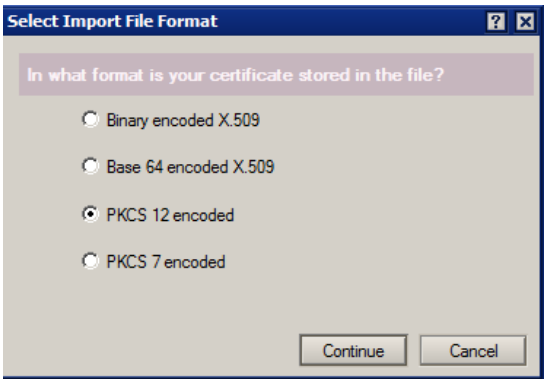
(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

c. Browse to the **.pfx** Internet certificate.



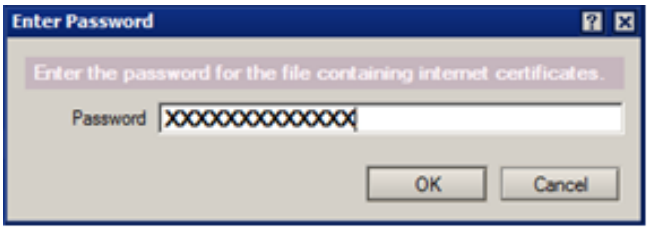
(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

d. On the **Select Import File Format** window, select **PKCS 12 encoded**, and then click **Continue**.



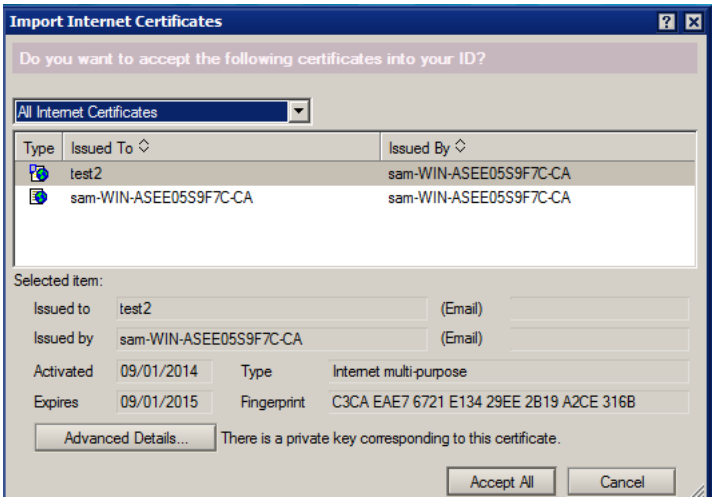
(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

e. On the **Enter Password** window, enter the password for the file containing the Internet certificate, and then click **OK**.



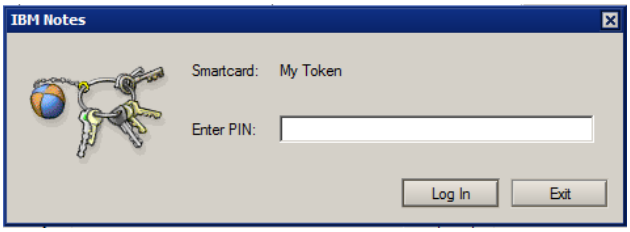
(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

f. On the **Import Internet Certificates** window, accept the certificate into the IBM Notes ID file, and then click **Accept All**.



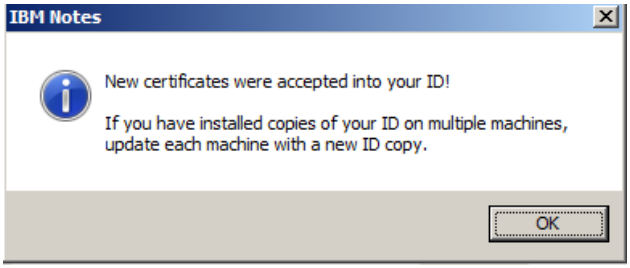
(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

g. This window is displayed because the token was enabled to secure the IBM Notes User ID. Enter the smart card PIN, and then click **Log In**.



(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

h. When this message is displayed, click **OK**. The Internet certificate is successfully imported.

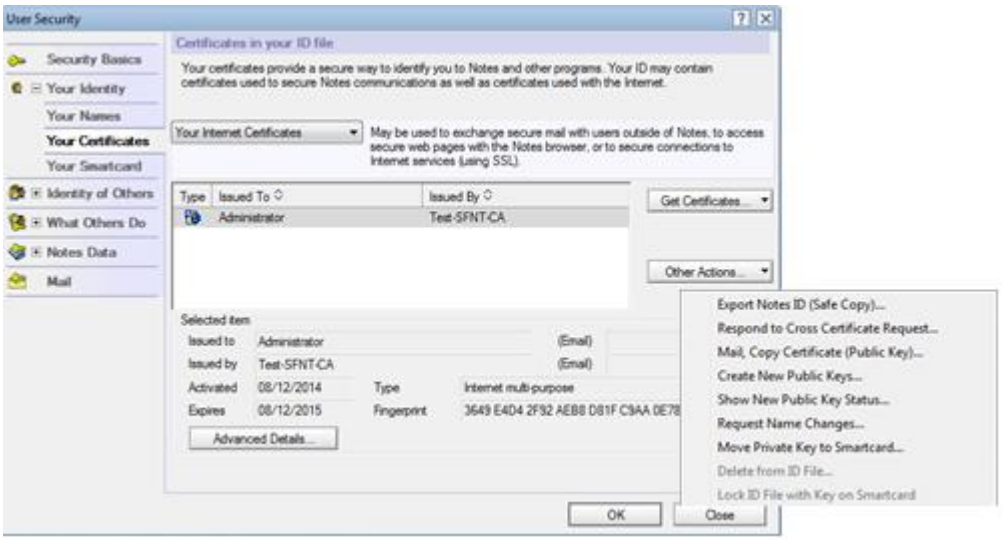


(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

6. On the **User Security** window, select **Your Identity > Your Certificates**. Complete the following steps, and then click **OK**.

a. Under **Certificates in your ID file**, click the **Your Internet Certificates** menu, and then select the certificate to use to secure the ID file.

b. Click the **Other Actions** menu, and then select Move Private Key to Smartcard.



(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

7. When this message is displayed, click **Yes**.

(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

8. Enter your smart card PIN to confirm the move.
9. When this message is displayed, click **OK**.

(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

Running the Solution

1. Launch IBM Notes and insert the configured token into the machine's USB port.
2. On the smart card log in window, from the **Smartcard** menu, select the applicable token name.

(The screen image above is from IBM® Notes® software. Trademarks are the property of their respective owners).

3. Enter your smart card PIN, and then click **Log In**.

APPENDIX

To import Internet certificates from a Smartcard

You can import Internet certificates and store them in the Lotus Notes ID file so that they can be found by, and used with, Lotus Notes.

NOTE: This option is only applicable to users who have enabled Smartcard login by securing the ID file with a secret.

1. Click **File > Security > UserSecurity**.
2. Enter your PIN when prompted.

   Note: If you are performing this step as part of enabling Smartcard login with an Internet certificate and key, you are not prompted for the PIN.

3. Click **Your Identity > Your Certificates.**
4. Click **Get Certificates**. A drop-down list appears, listing different ways of importing certificates into the ID file.
5. Select **Import Internet Certificate from a Smartcard**. This imports all available certificates from the current Smartcard.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	