



IDProtect Client for Linux

User Guide

Version 6
June 2014

www.athena-scs.com



Athena Smartcard Solutions, Inc.

SOFTWARE LICENSE AGREEMENT

READ THIS AGREEMENT CAREFULLY BEFORE CONTINUING WITH THE INSTALLATION OF THE SOFTWARE.

ALL USE OF SOFTWARE OF ATHENA SMARTCARD SOLUTIONS OR ANY OF ITS AFFILIATES (COLLECTIVELY, "ATHENA"), ARE AND SHALL BE SUBJECT TO THE TERMS AND CONDITIONS SET FORTH IN THIS AGREEMENT. BY INSTALLING THE SOFTWARE (AS DEFINED HEREUNDER) ON YOUR COMPUTER AND/OR BY USING THE SOFTWARE, YOU ARE ACCEPTING THIS AGREEMENT AND AGREEING TO BE BOUND BY ITS TERMS. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, YOU SHOULD PROMPTLY (WITHIN 7 DAYS FROM THE DATE YOU RECEIVE THIS PACKAGE) RETURN THE SOFTWARE TO ATHENA, UNOPENED. YOUR MONEY WILL BE REFUNDED.

1. **Title & Ownership.** THIS IS A LICENSE AGREEMENT AND NOT AN AGREEMENT FOR SALE. In consideration for a license fee, as shall be agreed, Athena hereby grants you, and you hereby accept, a personal, non-transferable, non-exclusive license ("License") to use the software component of Athena's product(s), including any revisions, corrections, modifications, enhancements and/or upgrades thereto (the "Software") and any other documentation or user guide related to the Software, shall remain Athena's property. All intellectual property rights (including, without limitation, copyrights, trade secrets, trademarks, patents etc.) evidenced by or embodied in and/or attached/connected/related to the Software (including, without limitation, the Software code, user guides and any other documentation) are and shall be owned solely by Athena. Nothing in this Agreement constitutes a waiver of Athena's intellectual property rights under any law.
2. **License.** You are granted a limited License to use the Software in executable form only, and only according to the terms of this Agreement: (1) you may install the Software and use it on computers located in your place of business; and (2) you are permitted to make a number of copies of the Software as defined in your sales agreement; ; however, any portion of the Software merged into another application shall be deemed as a derivative work belonging to Athena and will continue to be subject to the terms of this Agreement.
3. **Prohibited Uses.** Except as permitted in Sections 2 above, you agree not to (1) use, modify, merge or sub-license the Software except as expressly authorized in this Agreement; (2) sell, license (or sub-license), lease, assign, transfer, pledge, or share your rights under this License with/to anyone else; (3) modify, disassemble, decompile, reverse engineer, revise or enhance the Software or attempt to discover the Software's source code; (4) place the Software onto a server so that it is accessible via a public network; or (5) use any back-up or archival copies of the Software (or allow someone else to use such copies) for any purpose other than to replace an original copy if it is destroyed or becomes defective. If you are a member of the European Union, this Agreement does not affect your rights under any legislation implementing the EC Council Directive on the Legal Protection of Computer Programs. If you seek any information within the meaning of that Directive you should initially approach Athena.
4. **Limited Warranty.** Athena warrants, for a period of 3 months after the date of delivery to you (the "Warranty Period") that the Software, when and as delivered to you, will perform in substantial compliance with the user guide, provided that it is used on the computer hardware and with the operating system for which it was designed (the "Warranty"). The following are excluded from the Warranty: (i) insignificant defects, such as errors that can be easily corrected and will not show up as a performance defect; (ii) defects discovered in the Software that has been modified, altered, or enhanced without Athena's prior consent; and (iii) other damage caused by abuse, misuse, neglect, adjustment, or unauthorized repair or installation, or by the misuse of the Software.
5. **Warranty Disclaimer.** ATHENA DOES NOT GUARANTEE THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT ITS OPERATION WILL BE UNINTERRUPTED OR ERROR-FREE. TO THE EXTENT ALLOWED BY LAW, ATHENA EXPRESSLY DISCLAIMS ALL EXPRESS WARRANTIES NOT STATED HEREIN AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
6. **Limitation of Remedies.** In the event that at any time during the Warranty Period, a significant error is discovered in the Software, your exclusive remedy shall be for Athena to attempt, through reasonable efforts, to provide a correction for such error, free of charge. Warranty claims must be made in writing during the Warranty Period and within seven (7) days of the observation of the defect accompanied by evidence satisfactory to Athena.
7. **Exclusion Of Consequential Damages.** The parties acknowledge that the Software is inherently complex and may not be completely free of errors. EXCEPT IN RESPECT OF DEATH OR PERSONAL INJURY CAUSED BY ATHENA'S NEGLIGENCE, ATHENA SHALL NOT BE LIABLE (WHETHER UNDER CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE) TO YOU, THE USERS OF YOUR SOFTWARE PROGRAM OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE (INCLUDING INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES), INCLUDING, WITHOUT LIMITATION, ANY LOSS OR DAMAGE TO BUSINESS EARNINGS, LOST PROFITS OR GOODWILL AND LOST OR DAMAGED DATA OR DOCUMENTATION, SUFFERED BY ANY PERSON, ARISING FROM AND/OR RELATED WITH AND/OR CONNECTED TO ANY USE OF THE SOFTWARE, AND/OR YOUR SOFTWARE PROGRAM, EVEN IF ATHENA IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
8. **Limitation of Liability.** IN THE EVENT THAT, NOTWITHSTANDING THE TERMS OF THIS AGREEMENT, ATHENA IS FOUND LIABLE FOR DAMAGES BASED ON ANY SIGNIFICANT ERROR, ITS TOTAL LIABILITY SHALL BE LIMITED TO THE LICENSE FEE ACTUALLY PAID BY YOU FOR THE SOFTWARE.
9. **Termination.** Failure to comply with the terms of this Agreement shall terminate your License and this Agreement. Upon termination



of this License Agreement by Athena: (1) the License granted to you in this Agreement shall expire and you, upon termination, shall discontinue all further use of the Software; and (2) you shall promptly return to Athena all tangible property representing Athena's intellectual property rights and all copies thereof and/or shall erase/delete any such information held by you in electronic form. Sections 1, 4, 5, 6, 7, 8, 9 and 10 shall survive any termination of this Agreement.

10. **Governing Law & Jurisdiction.** This Agreement is governed only by the laws of Japan, and only the courts in Japan shall have jurisdiction in any conflict or dispute arising out of this Agreement.

By accepting this document you confirm the following statement:

I HAVE READ AND UNDERSTOOD THIS LICENSE AGREEMENT AND AGREE TO BE BOUND BY ALL OF THE TERMS.



Table of Contents

PREFACE	2
WHO SHOULD READ THIS MANUAL.....	2
PREREQUISITES.....	2
SUPPORTED VERSIONS	2
1. INSTALLING THE IDPROTECT CLIENT	4
1.2 INSTALLING THE IDPROTECT CLIENT USING .RPM FILES	4
1.3 INSTALLING THE IDPROTECT CLIENT USING .DEB FILES.....	8
1.4 ADVANCED INSTALLATION.....	10
1.5 REGISTERING ATHENA PKCS#11 AS A SECURITY MODULE IN FIREFOX.....	14
2. USING THE IDPROTECT FORMAT TOOL FOR PIN CARDS.....	16
3. USER PIN MANAGEMENT	25
CHANGING THE USER PIN.....	25
UNBLOCKING THE USER PIN	26
4. CHANGING THE ADMIN PIN/PUK.....	29
5. THE IDPROTECT MANAGER	31
6. COMPONENTS AND FILE LOCATIONS	33
FILES AND FILE LOCATIONS	33
SCRIPTS	34
ADDITIONAL TASKS PERFORMED BY THE SETUP.....	36
7. APPENDIX 1 – PREREQUISITES INSTALLATION.....	37
REDHAT & FEDORA SYSTEMS	37
CENTOS SYSTEMS	38
SUSE SYSTEMS.....	38
DEBIAN & UBUNTU SYSTEMS.....	39



Preface

IDProtect Client software is a set of utilities and middleware libraries which, coupled with an IDProtect LASER or ASECard Crypto smart card, provide support for Linux smart card services such as , secure e-mail, VPN, WEB SSL and support for most smart card aware third party applications using PKCS#11 standards.

Who Should Read This Manual

The guide is intended for IT managers, System Administrators, and Software engineers who are responsible for implementing smart card support in their organizations.

The guide assumes the reader is familiar with:

- General use of computers
- Mainstream Linux Distributions
- PKI and Digital Certificates

Prerequisites

This guide assumes the following prerequisites:

- **pcscd** installed and running on the Linux host. It is recommend setting the **pcscd** to automatic startup.
- CCID libraries are installed on the Linux host.
- pcsc-lite libraries are installed on the Linux host.
- openct and openct libraries **ARE NOT** installed on the Linux host. If openct and openct libraries are installed, they need to be removed from the Linux host.

Instructions for installing pccsd, ccid, pcsc-lite and corresponding libraries are detailed in Appendix A. The Appendix includes instructions and steps for locating and removing openct and related libraries.

Optional: The Athena PKCS#11 (libASEP11.so) module can be automatically registered by the installer (RPM or DEB files) as a security module in Firefox. The following prerequisites are required if the installer is to automatically register the Athena PKCS#11module:

- Install **Network Security Service tools** (Mozilla-nss-tools). The installation method and commands vary depending on the Linux Distribution used.
- Open Firefox once before the installation (during the IDProtect Client installation process Firefox must be closed).

Supported Versions

The IDProtect Client supports mainstream Linux Distributions and has been tested on the following Linux Distributions:

- Ubuntu 12.x and 13.x and 14 (X86 and X64)
- Fedora 17 and Fedora 18, Fedora 19 and Fedora 20 (X86 and X64)
- Debian 6 and Debian 7 (X86 and X64)



- Redhat 5.x and Redhat 6.x (X86 and X64)
- CentOS 5.x and CentOS 6.x (X86 and X64)
- SuSE 11 & OpenSuSE (X86 and X64)
- Mandriva 2011 (X86 and X64)

1. Installing the IDProtect Client

IDProtect Client is designed to work on mainstream Linux Distributions.

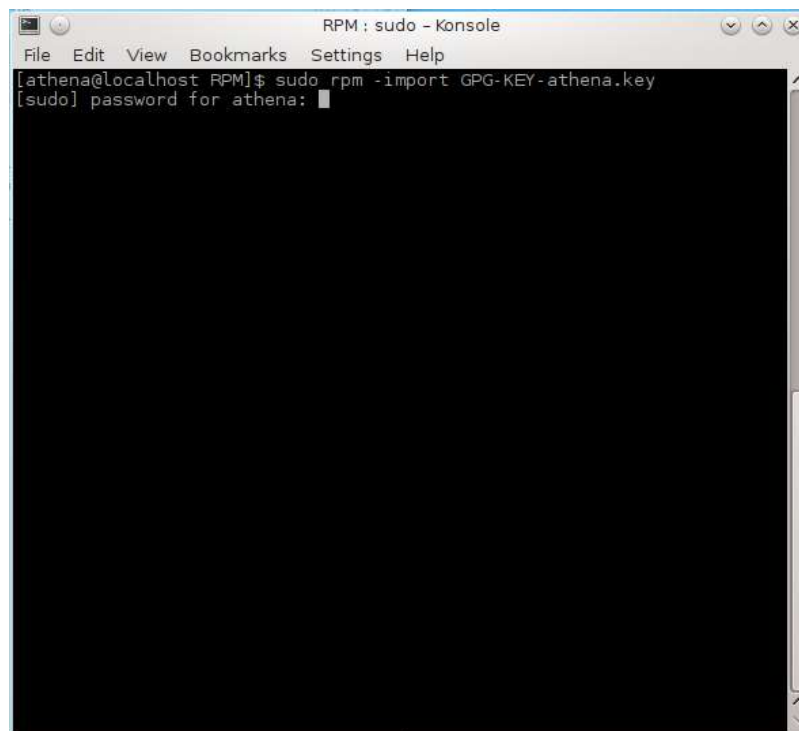
The IDProtect Client supports both x86 and x64 bit operating systems and the latest version/service packs of each operating system.

1.2 Installing the IDProtect Client using .rpm files

On certain Linux distributions installing using RPM requires the package to be verified such as when installing RPM packages on Fedora Linux with KDE Desktop.

If this is the case, the Athena Public signing key needs to be imported into the Linux system. The below steps were performed on a Fedora Linux. Steps required on other Linux distributions may vary.

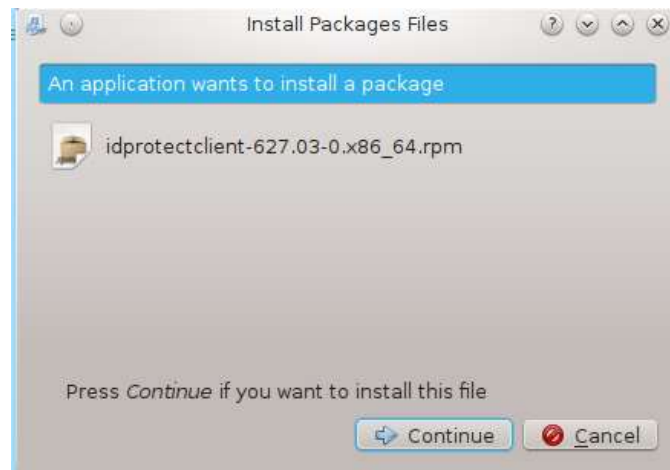
- Copy the **idprotectclient-627.03-0.i386.rpm** or **idprotectclient-627.03-0.x86_64.rpm** and **GPG-KEY-athena.key** to the Linux host.
- Open a terminal window in the above directory, type **sudo rpm --import </path-to-key>**, and enter the privileged (root) password when prompted.



Installing the RPM file

The below steps were performed on a Fedora Linux. Steps may vary on different Linux distributions.

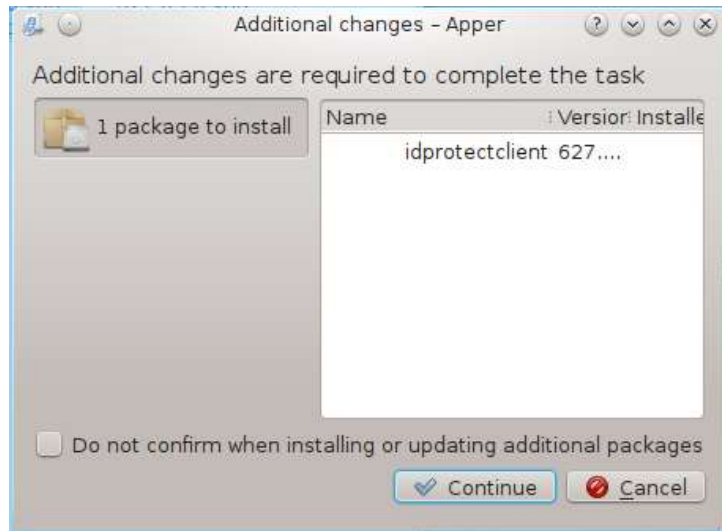
- Open the **idprotectclient-627.03-0.x86_64.rpm** and press **Continue** in the **Install Package Files**



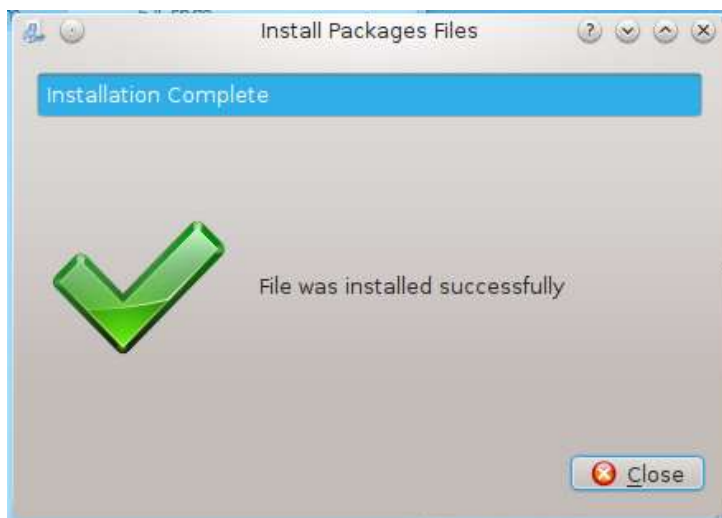
- Enter the a privileged (root) user password and press OK



- Let the installation run and approve additional tasks required by the RPM installer



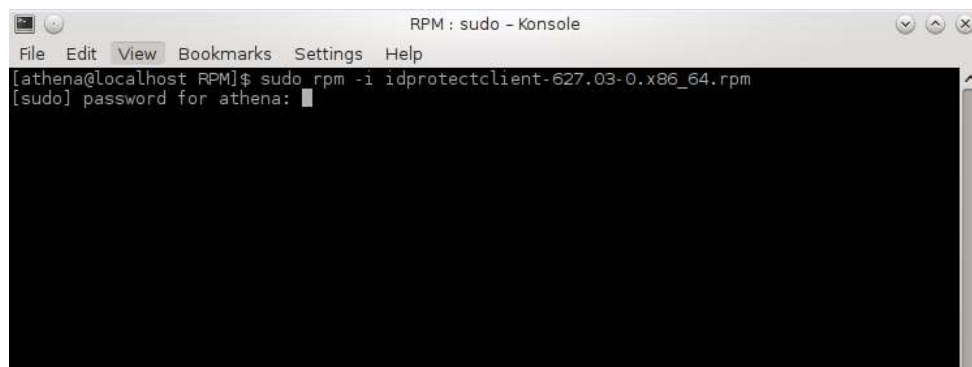
- Click **Close** when prompted by the installation.
- **Restart** the Linux host.



Note: RPM file may also be installed via scripts or from terminal windows. In this case, the RPM files is executed using the following command:

Sudo rpm -i idprotectclient-627.03-0.x86_64.rpm
or
Sudo rpm -i idprotectclient-627.03-0.i386.rpm

- When prompted enter a privileged (root) user password



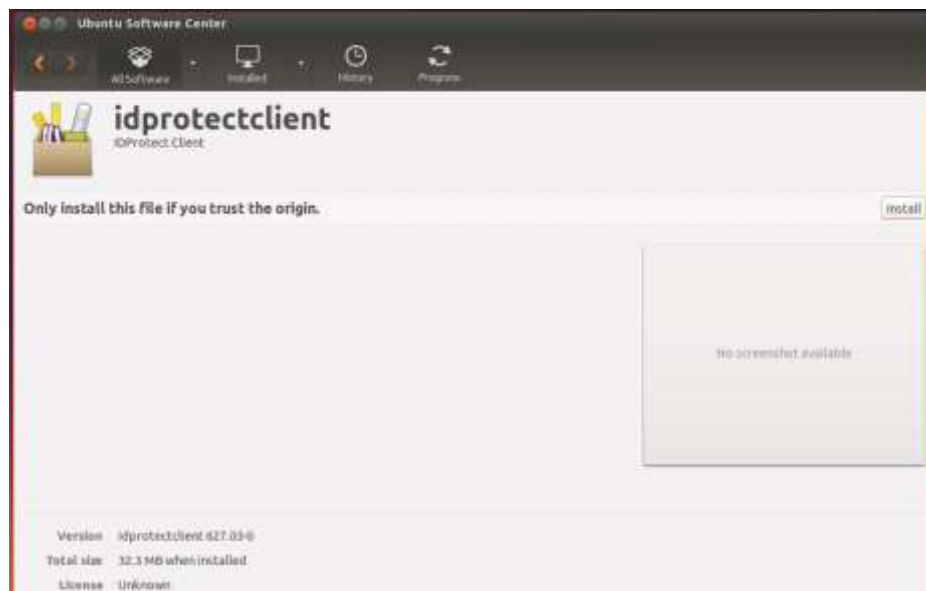
```
RPM : sudo - Konsole
File Edit View Bookmarks Settings Help
[athena@localhost RPM]$ sudo rpm -i idprotectclient-627.03-0.x86_64.rpm
[sudo] password for athena: 
```

- Let the installer perform the installation.
- **Restart** the Linux host.

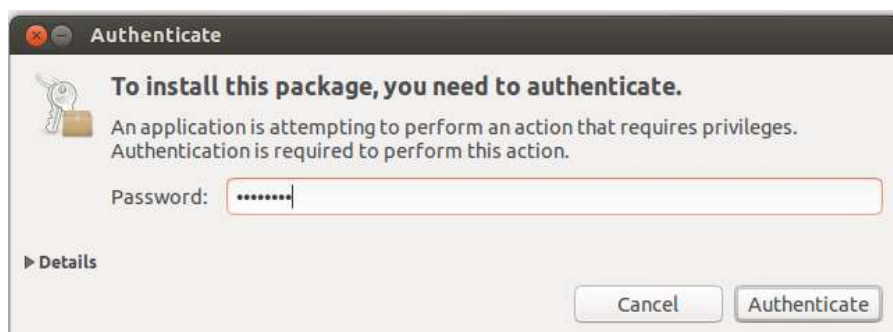
1.3 Installing the IDProtect Client using .deb files

The below steps were performed on Ubuntu Linux. Steps may vary on different Linux distributions.

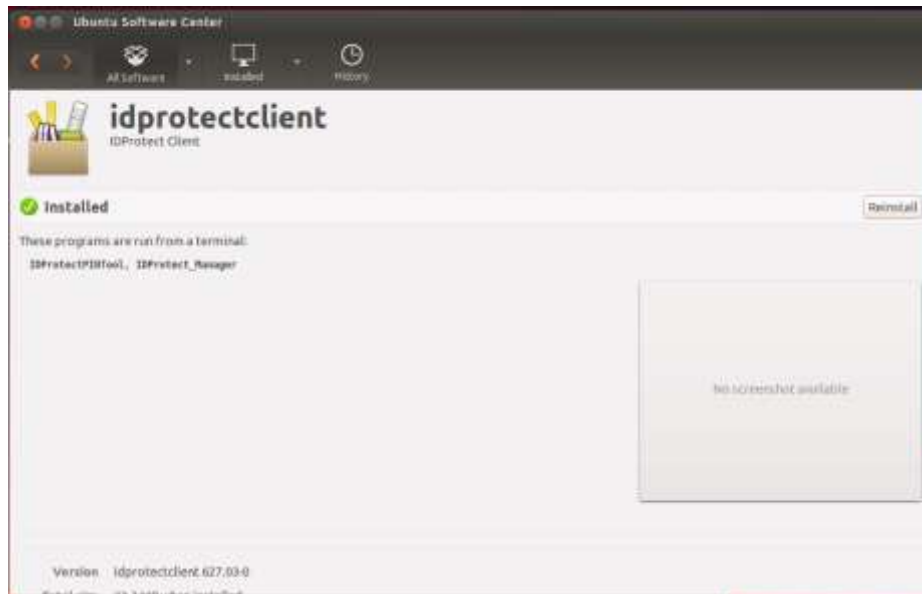
- Open **idprotectclient_627.03-0_i386.deb**. The DEB package will open in the Linux software installer application
- Click **Install**



- Enter privileged (root) user password when prompted and press **Authenticate**



- Let the installer perform the installation and close the Software installer when the installation is completed



- **Restart** the Linux host.

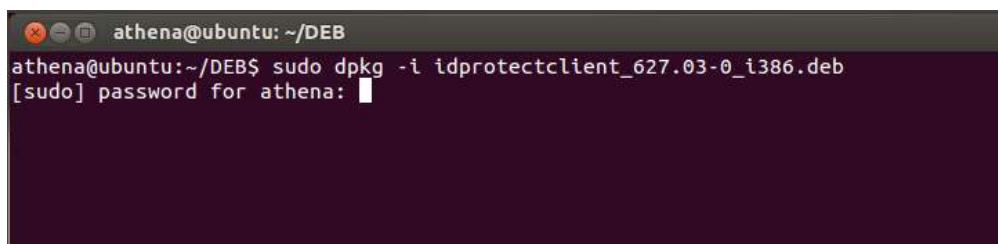
Note: DEB file may also be installed via scripts or from a terminal windows. In this case, the DEB files is executed using the following command:

Sudo dpkg -i idprotectclient-627.03-0.x86_64.deb

or

Sudo dpkg -i idprotectclient-627.03-0.i386.deb

- When prompted enter a privileged (root) user password



- Let the installer perform the installation.
- **Restart** the Linux host.

1.4 Advanced Installation

32 bit application running on x64 bit Linux host that require smartcard support, e.g. Adobe, need to use a 32 bit version of the IDProtect Client that can run on x64 platforms. In this case, in addition to installing the **idprotectclient627.03_x64** client on the Linux host, the **idprotectclient_lib_627.03_x86** needs to be installed on the Linux host.

Note: You must install `pcsc-lite-libs:i386 / libpcsclite1:i386` (relevant to the Linux Distribution you are using) in order to run the `Libs_x86` installation, without these components setup will not run.

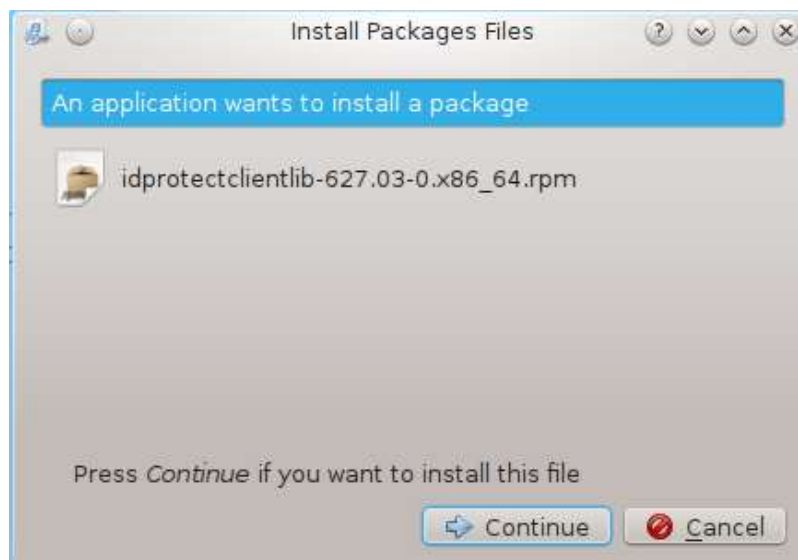
Note: **idprotectclient627.03_x64** **MUST** be installed on the Linux host before installing **idprotectclient_lib_627.03_x86**

Installing **idprotectclient_lib_627.03_x86** using rpm files

Note: If required follow section 1.3 to install Athena public signing key, **GPG-KEY-athena.key**

The below steps were performed on a Fedora Linux. Steps may vary on different Linux distributions.

- Open the **idprotectclientlib-627.03-0.x86_64.rpm** and press **Continue** in the **Install Package Files**



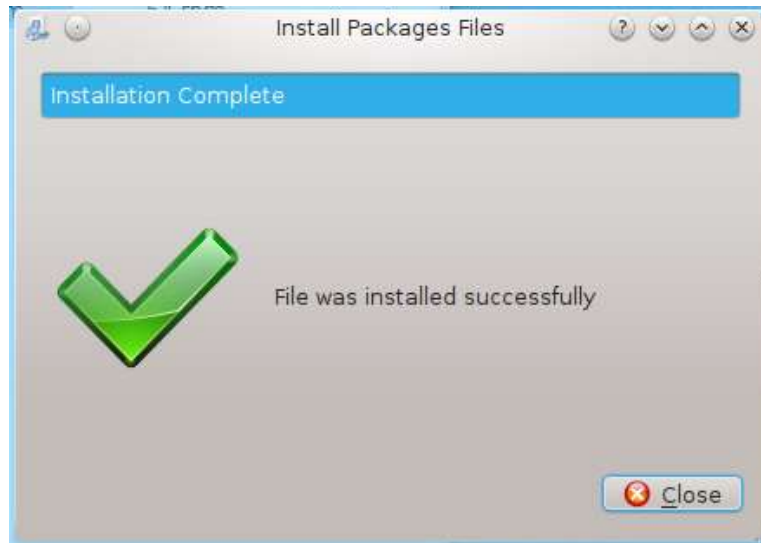
- Enter the a privileged (root) user password and press OK



- Let the installation run and approve additional tasks required by the RPM installer



- Click **Close** when prompted by the installation.

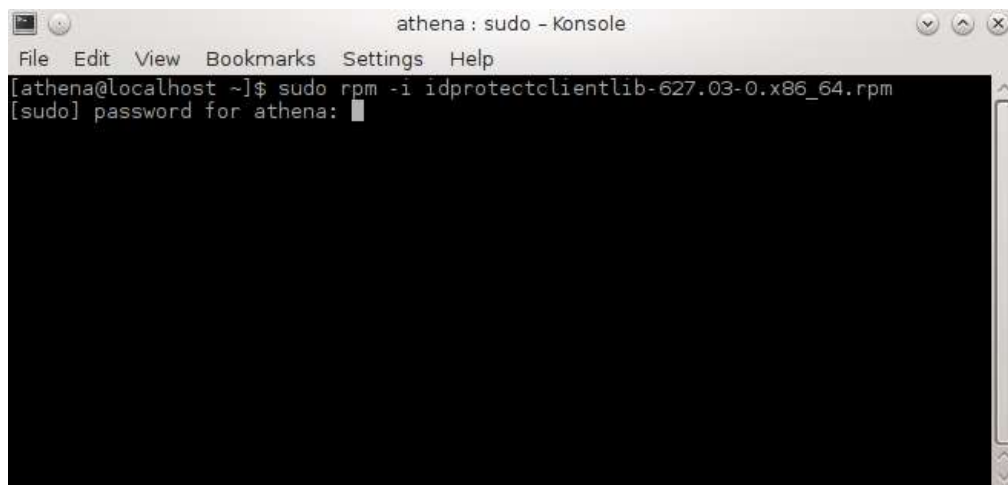


- **Restart** the Linux host.

Note: RPM file may also be installed via scripts or a terminal windows. In this case, the RPM files is executed using the following command:

Sudo rpm -i idprotectclientlib-627.03-0.x86_64.rpm

- When prompted enter a privileged (root) user password



- Let the installer perform the installation.
- **Restart** the Linux host.

Installing idprotectclient_lib_627.03_x86 using deb files

The below steps were performed on Ubuntu Linux. Steps may vary on different Linux distributions. Double-click the idprotectclientlib_627.03-0_amd64.deb and click **Install** when requested



- Enter privileged user password when requested and click **Authenticate**



- Let the installer perform the installation and close the Software installer when the installation is completed.
- **Restart** the Linux host.

Note DEB file may also be installed via scripts or a terminal windows. In this case, the DEB files is executed using the following command:

Sudo dpkg -i the idprotectclientlib_627.03-0_amd64.deb

- When prompted enter a privileged (root) user password

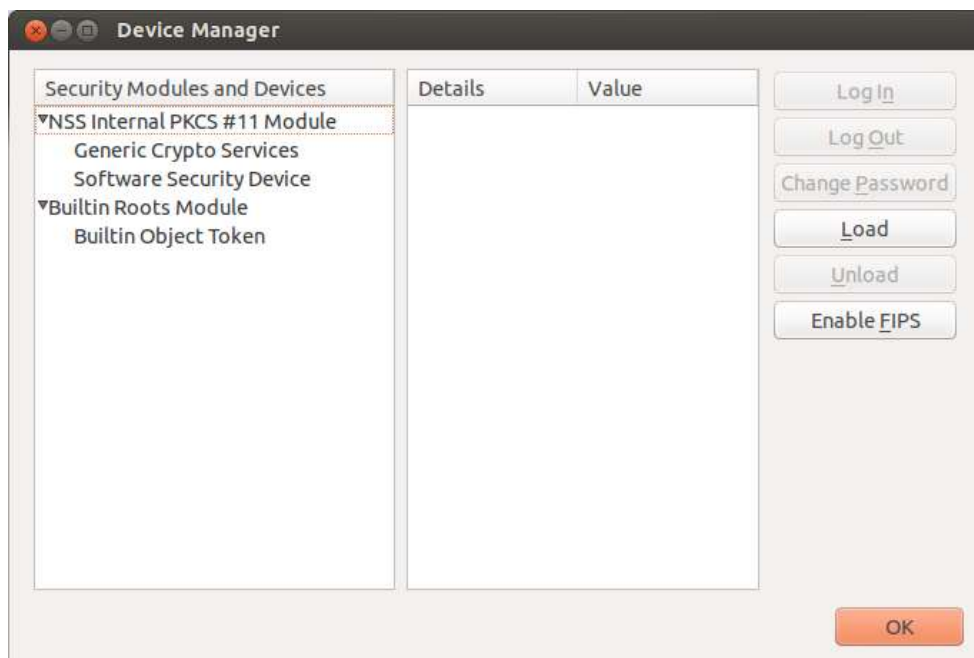
```
athena@ubuntu:~$ sudo dpkg -i idprotectclientlib_627.03-0_amd64.deb
[sudo] password for athena: 
```

- Let the installer perform the installation.
- **Restart** the Linux host.

1.5 Registering Athena PKCS#11 as a security module in Firefox

The steps below are performed on Ubuntu 13.

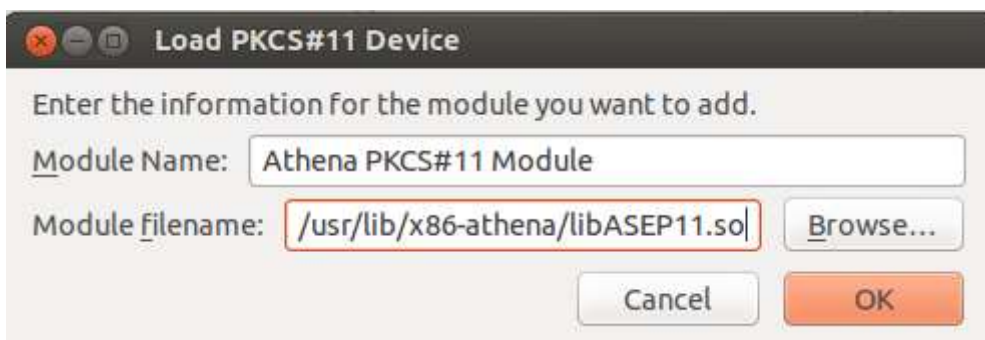
- In Firefox, go to **Edit > Preferences > Advanced > Certificates > Security Devices**



- Click **Load** to open the security module loading wizard



- Enter **Athena PKCS#11 Module** as the Module Name
- Enter **/usr/lib/x86-athena/libASEP11.so** as the Module Filename **or** **/usr/lib/x64-athena/libASEP11.so** (Depending on your Linux OS architecture).
- Click **OK**



2. Using the IDProtect Format Tool for PIN Cards

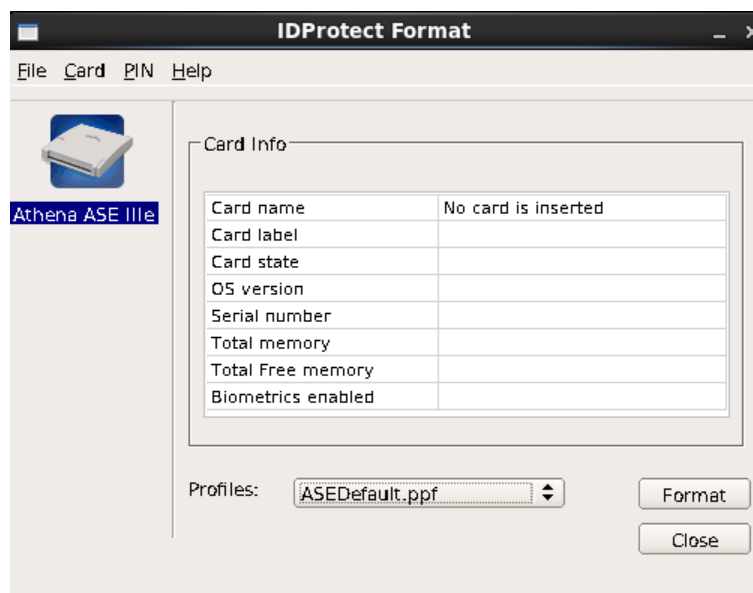
The **IDProtect Format** tool is an easy to use application that provides the Administrator with full control over the card security policy and various card parameters. The tool can be used to:

- View card details such as *Serial Number*, *Free memory space*, etc.
- Manage the User and Admin PINs and other parameters without invalidating the credentials stored on the card.
- Viewing, editing and creating new *Format Profiles*.
- Formatting and reformatting cards.
- Wiping the card (bringing back the card to a non-formatted state)

To start the **IDProtect Format** tool:

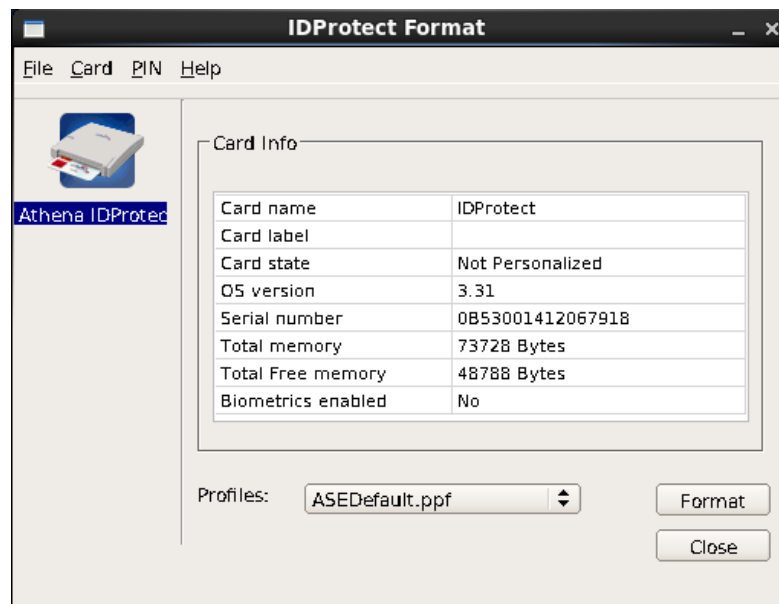
Click **IDProtect Format** on the desktop shortcut or from the application group.

The **IDProtect Format** window appears:

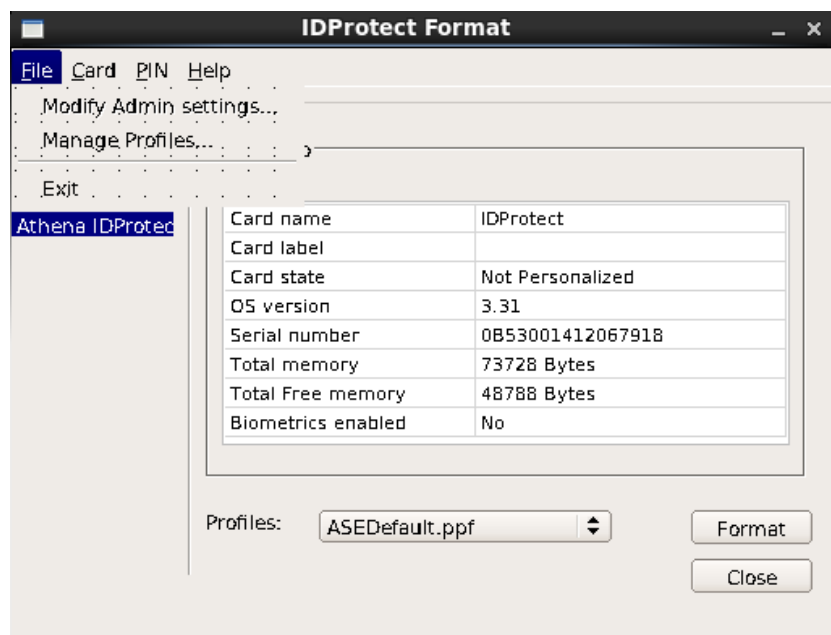


- Insert an Athena smart card or token into an installed smart card reader to begin working with the **IDProtect Format**.

The **IDProtect Format** tool window will display the inserted card details and the smart card reader/token picture, on the left side of the window, will indicate that a card is inserted.



- In order to format a card:
 - Select the required *Format Profile* from the *Profile* pop-up list.
 - Click the **Format** button.
 - Note: If you are re-formatting a previously formatted card, you will be prompted to enter the **Admin PIN**. ('00000000' is the value used in the ASEDefault profile).
 - Wait for the "Success" message.
- If you would like to review, add, remove, or edit a format profile, select the **Manage Profiles...** item from the **File** menu.



The **Profile List** window appears:



You may now **select** the *required format* profile and click **Modify...** to modify or review the personalization parameters or click **New...** to create a new profile. Clicking **Remove** will delete the selected profile.

Clicking **Modify...** or **New...** will launch the **Manage Profile** window.

Notes:

- The *ASEDefault.ppf* profile cannot be deleted. It can only be saved under a different name.
- Profiles are saved under `/etc/Athena/ppf`. They are not visible from other accounts, unless they are manually copied there.

The **Manage Profile** window is where you set the security policy and relevant parameters for cards that you plan to format. There are 3 separate tabs – **General**, **User PIN** and **Admin PIN**.

I. General Tab

The screenshot shows the 'Manage Profiles' window with the 'General' tab selected. The window has a title bar with a close button. Inside, there are three tabs: 'General', 'User PIN', and 'Admin PIN'. The 'General' tab contains the following fields and options:

- Profile name:** A text box containing 'NewProfile1.ppf'.
- Card Info:** A group box containing:
 - Card label:** An empty text box.
 - ☐ change User PIN at first use
 - ☐ Must change user PIN after unlock
 - ☐ Stays valid for: 60 Min
 - ☐ Expires after: 30 Days
 - ☒ Remember last: 1 PINs
- Buttons:** 'Save' and 'Cancel' buttons at the bottom right.

Profile Name – Lets you set a name for a new profile or modify an existing profile name.

Card Info

Card Label – The Card Label is used in order to help you identify the cards you format. The label has no effect on any of the smart card services. It is equivalent to the *PKCS#11 Token Label*. If not set by you, the label will automatically default to the "ASECard + Card serial number" or

"IDProtect + Card serial number" or "CNS + Card serial number" depending on the type of card you are using.

Change PIN at first use– The user will be prompted to change the **User PIN** the first time a card is used. Aside from changing the PIN, no other PIN protected smart card enabled action will be allowed until the PIN is changed to a new value.

Must change user PIN after unblock– During the unblock procedure; a new PIN value is selected. Choosing this option will require the user to change the User PIN again during the next use of the card.

Stays valid for X Minutes– sets the duration in which a verified **User PIN** stays valid. Once X minutes passes, the user will be asked to verify the PIN again.

Expires after X Days – Forces the user to change his PIN every X days.

Remember last X PINs – Enforces a policy whereby a new PIN cannot be equal to one of the last X PIN values used (up to 16 last values can be stored on the card. For security reasons, only a HASH of the old PIN is stored).

II. User PIN Tab

The screenshot shows a window titled "Manage Profiles" with a close button (X) in the top right corner. Inside the window, there are three tabs: "General", "User PIN" (which is selected and highlighted with a blue underline), and "Admin PIN". The "User PIN" tab contains the following elements:

- A label "PIN policy" above a dropdown menu showing "Default".
- A label "PIN Value" above a text input field containing "11111111".
- A button labeled "Complexity rules..." below the PIN Value field.
- At the bottom right of the window, there are two buttons: "Save" and "Cancel".


PIN Value

You may select from the pop-up menu, 3 methods to set PINs during personalization:

- **Manual** - you will be automatically prompted to enter the **User PIN** during the formatting process of each card.
- **Default** - Each card will be formatted with the default **User PIN** as specified in the Profile.
- **Random** - A random PIN will be generated during the formatting of the card and will be presented to you. You must copy this PIN and save it in a safe place.

Note: If you choose **Random** PIN generation, you must copy the PIN value from the screen and save it in a safe place. There is no way to recover a **Random** PIN, aside from noting it down.

Random PINs are generated according to the PIN complexity rules as set below. For example, when choosing a **Random User PIN** value, the following dialog will appear during personalization of the card.

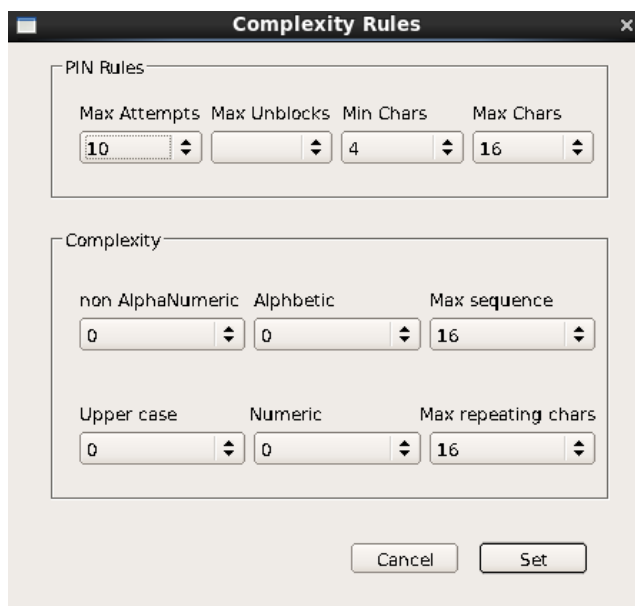


The image shows a 'Set PIN' dialog box with a title bar containing a close button. It is divided into two sections: 'User' and 'Admin'. The 'User' section has a 'User PIN' field containing the text 'FWHZMfdvsvFLRwrl' and an empty 'Confirm User PIN' field. The 'Admin' section has empty 'Admin PIN' and 'Confirm Admin PIN' fields. At the bottom, there is a message: 'Please make sure to copy and backup the randomly generated User PIN in a safe place!' and two buttons, 'Set' and 'Cancel'.

Make sure to match the choice of PIN generation options, to your organization security policy.

Complexity Rules

Enable you to apply various rules to the **User PIN**, according to your organization security policy.



The image shows a 'Complexity Rules' dialog box with two main sections: 'PIN Rules' and 'Complexity'. The 'PIN Rules' section contains four spinners: 'Max Attempts' (set to 10), 'Max Unblocks' (empty), 'Min Chars' (set to 4), and 'Max Chars' (set to 16). The 'Complexity' section contains six spinners arranged in two rows. The first row has 'non AlphaNumeric' (0), 'Alphabetic' (0), and 'Max sequence' (16). The second row has 'Upper case' (0), 'Numeric' (0), and 'Max repeating chars' (16). At the bottom are 'Cancel' and 'Set' buttons.

PIN Rules			
Max Attempts	Max Unblocks	Min Chars	Max Chars
10		4	16

Complexity		
non AlphaNumeric	Alphabetic	Max sequence
0	0	16
Upper case	Numeric	Max repeating chars
0	0	16

Buttons: Cancel, Set

Max Attempts – The number of unsuccessful consecutive verification attempts, before the **User** PIN is blocked.

Max Unblocks - The number of successful **User PIN** unblocks allowed during the life of a card. Reaching the maximum number will require re-formatting of the card.

Min and Max chars - sets the required length of the **User** PIN.

- You may change any of these parameters in the **Manage Profile** window to suit your security policy. Once you have finished editing, you may save the profile under the same name, replacing the previously saved profile or save it under a different name (recommended). If you click **Cancel**, any changes made to the current profile will be lost.

Once you decide to use a specific profile for card formatting, select it from the Profile pop-up list in the main **Format Tool** window and click **Format**.

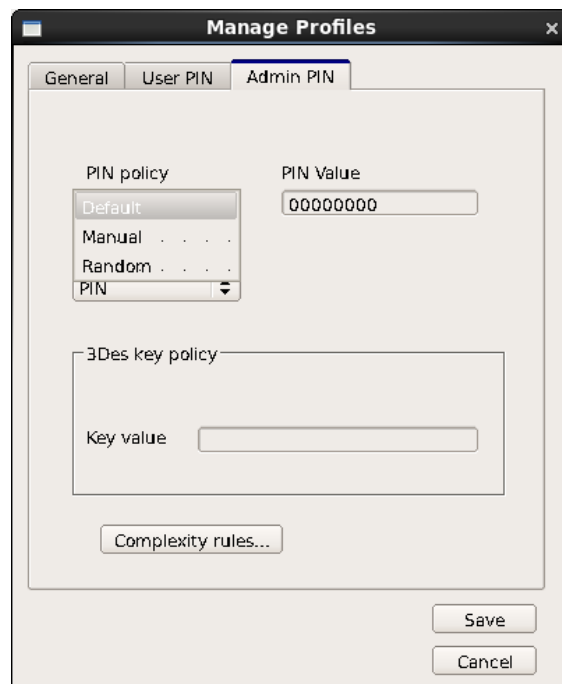
III. ADMIN PIN Tab

The screenshot shows a window titled "Manage Profiles" with three tabs: "General", "User PIN", and "Admin PIN". The "Admin PIN" tab is selected. Inside the tab, there are two dropdown menus: "PIN policy" set to "Default" and "Verification type" set to "PIN". To the right of these is a text field labeled "PIN Value" containing "00000000". Below these is a section titled "3Des key policy" which contains a "Key value" text field. At the bottom of this section is a button labeled "Complexity rules...". At the bottom right of the dialog are "Save" and "Cancel" buttons.

Using the **Admin PIN** tab is similar to the **User PIN** tab.

Setting the **Max attempts** on the Admin PIN has important consequences since once the Admin PIN is blocked, the card cannot be used any more.

Warning: Once the Admin PIN is blocked, the card can be still be used but any action requiring the Admin PIN such as User PIN Unlock and Formatting will fail.



When setting the Admin PIN to be a 3DES key, the entered key value should be a valid DES/3DES key value, i.e. 8, 16 or 24 bytes hex (16, 32 or 48 digits) input.

3. User PIN management

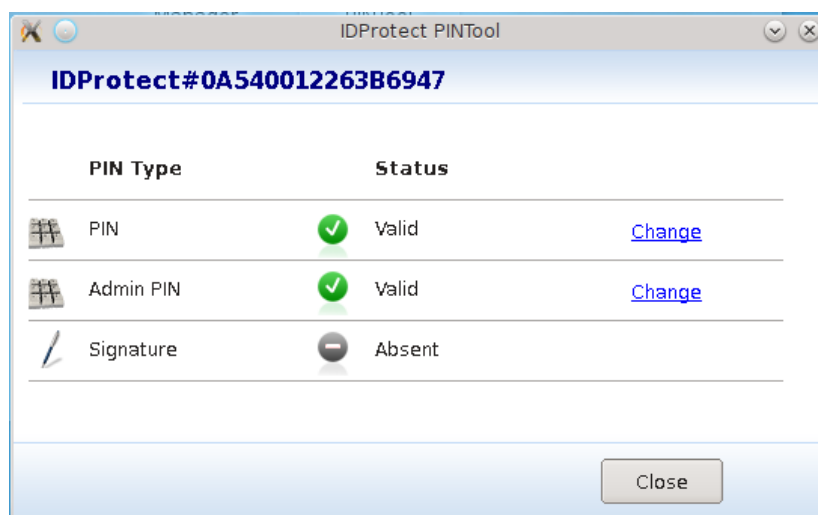
The below section explains in step-by-step stage how to change a User PIN or Unblock a User PIN.

Changing the User PIN

It is possible to change the **User** and **Admin PINs** without re-personalizing the card. There are several ways to access the Change/Unblock PIN tools.

The End User may change the **User PIN** of their card at any time by following this procedure:

- Open the **IDProtect PINTool** from the desktop shortcut link on the desktop or opening the **IDProtect PINTool** from the Application group. The IDProtect PINTool can be launched from the **IDProtect Manager > PIN** menu
- The **IDProtect PIN Tool** window will appear.



- Click the **Change** link. The IDProtect Change User PIN dialog will appear. Enter the current User PIN and Confirm the new User PIN.



(The **User PIN** of the Athena default profile is '1111111')

- When completed, the following dialog will appear:



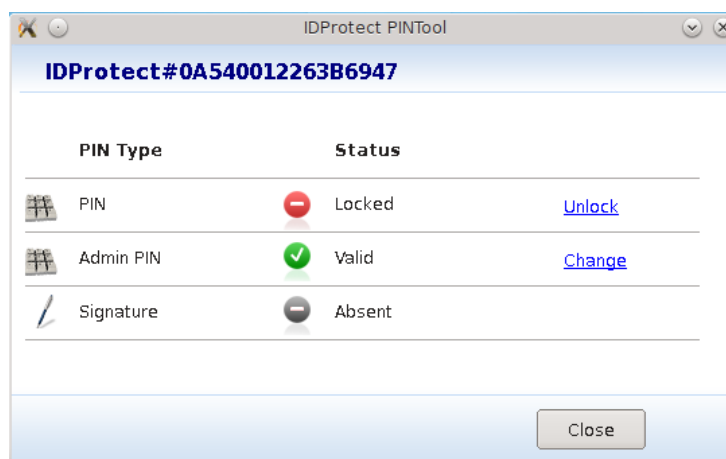
Please note: If the user enters a wrong **User PIN** several times, until the Maximum Attempts number is reached (default max attempts is 10), he/she will block the card and will no longer be able to communicate with it. In order to have access to the card again, the **User PIN** will have to be unblocked using the **Admin PIN**.

Unlocking the User PIN

When a user enters a wrong PIN value several times, until the Max Attempts parameter which was set during the card personalization (the default is 10 attempts) is reached, the **User PIN** becomes blocked and can only be unblocked using the **Admin PIN**.

- Open the **IDProtect PINTool** from the desktop shortcut link on the desktop or opening the **IDProtect PINTool** from the Application group. The IDProtect PINTool can be launched from the **IDProtect Manager > PIN** menu

- The **IDProtect PIN Tool** window will appear.



- Press the **Unlock** link, enter the required information and press **OK**



- The Administrator will now have to enter and confirm a new value for the **User PIN**.
- If the **Admin PIN (PUK)** is entered incorrectly, the following message will appear:



Note: After 2 additional (unsuccessful) attempts (or as set in the Max Attempts parameter for the **Admin PIN** in the profile) the card will become blocked. Once blocked the card **cannot** be used or re-personalized.

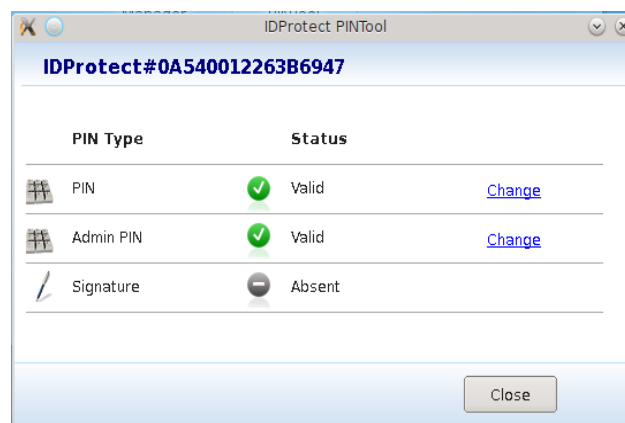
- Press OK when notified the User PIN has been unlocked.



4. Changing the Admin PIN/PUK

It is possible to change the **Admin PIN/PUK** without re-personalizing the card. There are several ways to access the Change/Unblock PIN tools.

- Open the **IDProtect PINTool** from the desktop shortcut link on the desktop or opening the **IDProtect PINTool** from the Application group, or
- The **IDProtect PIN Tool** window will appear.



- Select the **Change** link next to the Admin PIN Status. The **IDProtect Change Admin PIN** dialog will appear. Enter the current **Admin PIN** and afterwards the **New Admin PIN** and **Confirm New PIN**, and press **Change**.



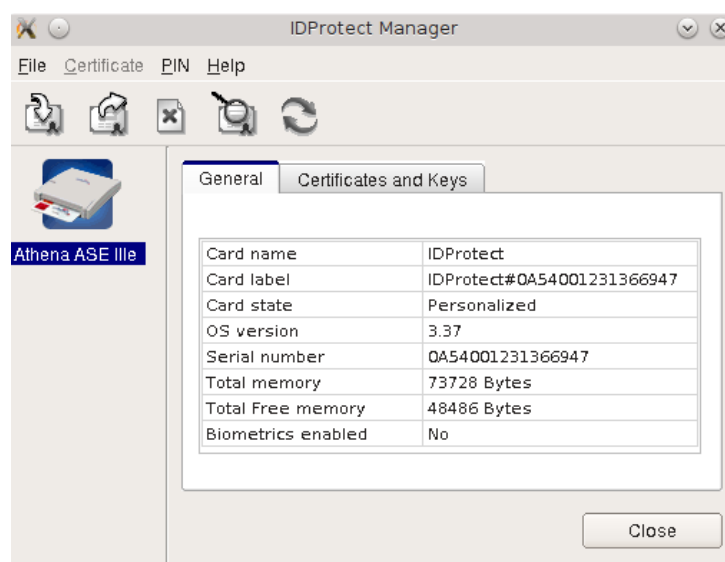
- Press **OK** when the PIN changed dialog appears.



5. The IDProtect Manager

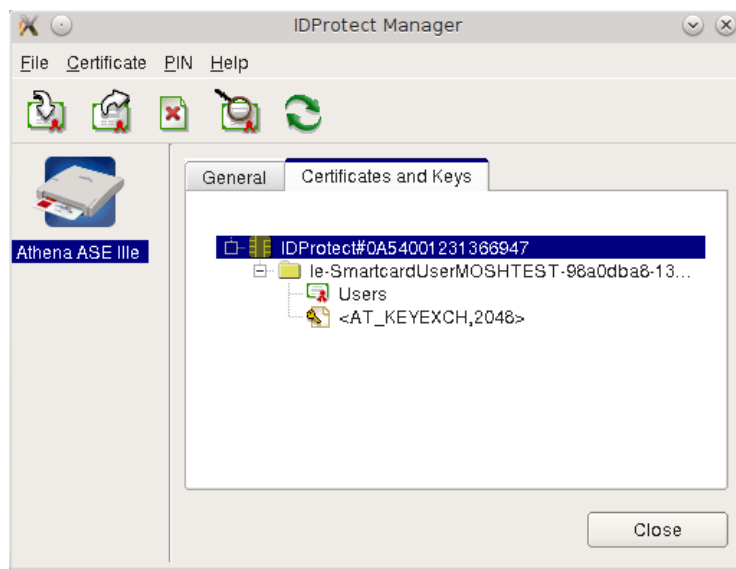
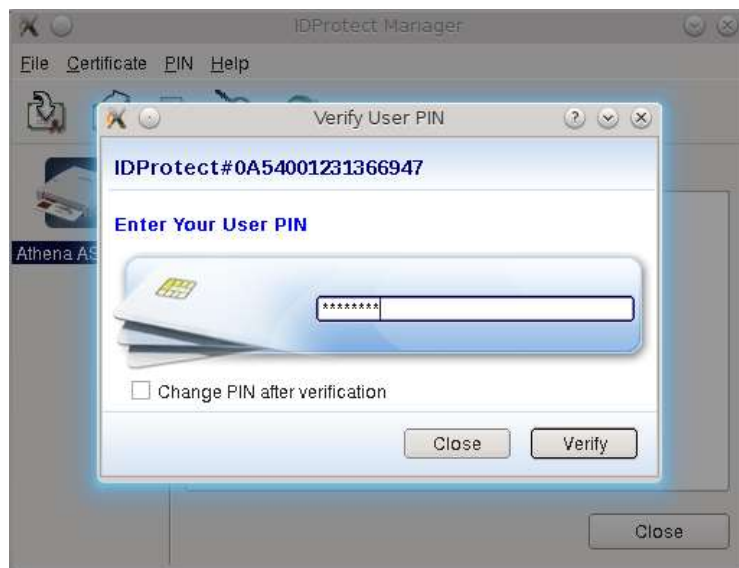
The **IDProtect Manager** is the central utility used to manage the card and view information related to the card, certificate and keys.

Open the **IDProtect Manager** from the desktop shortcut link on the desktop or opening the **IDProtect Manager** from the Application group.



IDProtect Manager displays the inserted card's information and enables managing of the **User PIN** and viewing details about certificates and keys stored on the card.

Clicking on the **Certificates & Keys** tab will display information and enable managing of certificates, following verification of the User PIN.



You can use the drop down menus, Toolbar Icons, or right-click menu to perform the following operations on the card:

- **Exporting certificates** – enables exporting of a certificate using the .cer format.
- **Deleting objects** - most objects can be deleted, unless they are part of a Default Container. Parts of a Default Container can be deleted only after designating another container as Default.
- **Viewing certificate information** – Double clicking on the certificate open the certificate for viewing.
- **Refreshing the display**
- **Manage the PINs** – Access the IDProtect PINTool from the **PIN** to manage the User PIN or Admin PIN

6. Components and File locations

Files and file locations

libQtGui.so.4

Installed at:

/usr/lib/x86-athena or /usr/lib/x64-athena

Functionality:

Enables the use of GUI for our applications, we use as shared library located at one known place.

libQtCore.so.4

Installed at:

/usr/lib/x86-athena or /usr/lib/x64-athena

Functionality:

Enables the use of GUI for our applications, we use as shared library located at one known place.
This library is dependency for QtGui.

libASEP11.so

Installed at:

/usr/lib/x86-athena or /usr/lib/x64-athena

Functionality:

Provides support for PKCS#11 applications, such as PGP, Netscape, Mozilla and many more.

IDProtectPINTool

Installed at:

/usr/bin

Functionality:

Allows changing or unlocking the PIN. It has full functionality such as the Windows IDProtect PinTool. Including support for Admin cards operations.

IDProtectPINTool.png

Installed at:

/usr/bin

Functionality:

PNG image for the desktop shortcut.

IDProtectManager

Installed at:

/usr/bin

Functionality:

Allows managing certificates and keys on the smart card.

IDProtectManager.png

Installed at:

/usr/bin

Functionality:

PNG image for the desktop shortcut.



AthenaLogo.png

Installed at:

/usr/bin

Functionality:

PNG image for the desktop directory.

IDPClientDB.xml (current user)

Installed at:

~/.ase

Functionality:

XML file which reflects the current user registry entry (HKEY_CURRENT_USER) of the Windows IDProtect Client. This gives a very comfortable way to control IDPC settings.

IDPClientDB.xml (local machine)

Installed at:

/etc/Athena

Functionality:

XML file which reflects the local machine registry entry (HKEY_LOCAL_MACHINE) of the Windows IDProtect Client.

Athena-IDProtectClient.desktop, Athena-IDProtectManager.desktop

Installed at:

/usr/share/applications

Functionality:

Provides the desktop shortcut properties.

Athena-IDProtectClient.directory

Installed at:

/usr/share/desktop-directories

Functionality:

Provides desktop short cut directory properties. Use to create applications directory folder for Athena.

EditPinfoList.out

Installed at:

/usr/bin/Athena

Functionality:

Application run by InstallDevices script with parameters for Athena CCID devices. (Described in CCID Athena devices).

Scripts

Postflight

Installed at:

/usr/bin/Athena

Functionality:

- Installs Athena and JaCarta CCID devices (Described in CCID Athena devices).



- Set the desktop folder and shortcut for IDProtect PINTool.
- Remove old entries of "Athena PKCS#11 Module" from Firefox.
- Installs new entry "Athena PKCS#11 Module" to Firefox.

Manager and PinTool

Installed at:

/usr/bin /Athena

Functionality:

Set the desktop shortcuts for the tools.

Mozilla

Installed at:

/usr/bin /Athena

Functionality:

Installs libASEP11.so to Mozilla Firefox.

uninstall

Installed at:

/usr/bin /Athena

Functionality:

- Removes entries of "Athena PKCS#11 Module" from Firefox.
- Removes the Desktop entry for IDProtect PINTool.



Additional tasks performed by the setup

Add CCID devices to Info.plist

Installed at:

/usr/lib/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist (for x86 OS)

/usr/lib64/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist (for x64 OS)

(note locations may change depending Linux Distribution)

Functionality:

We check for 6 devices and if they do not appear in the Info.plist we add them.

Devices:

VID	PID	Device friendly name
0x0DC3	0x1004	Athena ASEDrive CCID
0x0DC3	0x1007	Athena ASEDrive IIe KB BIO-PIV
0x0DC3	0x0900	Athena IDProtect Key
0x0DC3	0x1102	Athena ASEDrive IIe KB
0x0DC3	0x100F	Athena ASEKey CCID
0x24DC	0x0101	ARDS JaCarta

Uninstall IDProtect for Linux

Functionality:

The installer creates and uninstall file at: [InstallationFolder]\uninstall. The uninstall cleans all install actions.

Check installed components

Functionality:

The installer checks if the following components are installed: pcscd, If pcscd (Manages smart cards and readers) is not installed the setup will exit with an error message.

7. Appendix 1 – prerequisites installation

The purpose of this appendix is to provide the steps required to install pcsc, ccid and pcsc-lite components and libraries required by the IDProtect Client. Additionally If you have installed two CCID drivers (OpenCT, pcsc-lite and ccid), they may compete for resources. openct needs to be removed. The appendix details how to remove openct and its related libraries.

Throughout the instructions and steps below it is important to first remove openct and only the install pcsc, CCID and pcs-lite components and libraries.

Note It is the user's responsibility to make sure applications that may rely on openct are not affected by the removal of openct and its related libraries.

Note Throughout the installation of pcsc, CCID and pcs-lite components, the "-y" means the installation will not prompt the user to acknowledge the installation but rather continue with the installation once all required packages are identified. Should user acknowledgment be require the same commands can be used without the "-y" option.

Redhat & Fedora systems

1. Remove openct -

Verify if openct is installed-
In terminal run **rpm -qa | grep openct**
Below are the results return if openct is installed:

```
pcsc-lite-openct-<version_number>  
openct-devel-< version_number>  
openct-< version_number>
```

Note: results may vary slightly between different Linux distributions

2. Remove the openct components listed above in step 1 by running the following commands in a terminal window:

```
sudo rpm -e pcsc-lite-openct  
sudo rpm -e openct-devel  
sudo rpm -e openct
```

You may need to use -nodeps if there are dependencies, e.g.
sudo rpm -e - nodeps openct

3. Install PCSC, CCID and pcs-lite

Run the following command in terminal window – **sudo yum install -y ccid**
Run the following command in terminal window – **sudo yum install -y pcsc-lite**



CentOS systems

1. Remove openct

Verify if openct is installed-

In terminal run **rpm -qa | grep openct**

Below are the results return if openct is installed:

```
pcsc-lite-openct-<version_number>  
openct-devel-< version_number>  
openct-< version_number>
```

Note: results may vary slightly between different Linux distributions

2. Remove the openct components listed above in step 1 by running the following commands in a terminal window:

```
sudo rpm -e pcsc-lite-openct  
sudo rpm -e openct-devel  
sudo rpm -e openct
```

You may need to use `-nodeps` if there are dependencies, e.g.

```
sudo rpm -e - nodeps openct
```

3. Install PCSC, CCID and pscs-lite

Run the following command in terminal window – `sudo yum install -y ccid`

Run the following command in terminal window – `sudo yum install -y pcsc-lite`

SuSE systems

1. Remove openct

Verify if openct is installed-

In terminal run **rpm -qa | grep openct**

Below are the results return if openct is installed:

```
pcsc-lite-openct-<version_number>  
openct-devel-< version_number>  
openct-< version_number>
```

Note: results may vary slightly between different Linux distributions

2. Remove the openct components listed above in step 1 by running the following commands in a terminal window:

```
sudo rpm -e pcsc-lite-openct  
sudo rpm -e openct-devel  
sudo rpm -e openct
```



You may need to use `-nodeps` if there are dependencies, e.g.
`sudo rpm -e - nodeps openct`

3. Install PCSC, CCID and pscs-lite

Run the following command in terminal window – **`sudo zypper install -y pcsc-ccid`**
Run the following command in terminal window – **`sudo zypper install -y pcsc-lite`**

Debian & Ubuntu systems

1. Remove openct

Verify if openct is installed-
In terminal run `dpkg-query -f | grep openct`
Below are the results return if openct is installed:

ii libopenct1	0.6.20-1.1	middleware framework for smart
card terminals (libraries)		
ii openct	0.6.20-1.1	middleware framework for smart
card terminals		

Note: results may vary slightly between different Linux distributions

2. Remove the openct components listed above in step 1 by running the following commands in a terminal window:

```
sudo apt-get remove -y openct
sudo apt-get remove -y libopenct1
```

3. Install PCSC, CCID and pscs-lite

Run the following command in terminal window **`sudo apt-get install -y pcscd`**
Run the following command in terminal window **`sudo apt-get install -y libccid`**
Run the following command in terminal window **`sudo apt-get install -y libpcsc-lite`**