Becrypt
DISK Protect CPA

Secured by RSA Implementation Guide for SecurID Authenticators

Last Modified: December 17, 2014

Partner Information

Product Information	
Partner Name	Becrypt Ltd
Web Site	www.becrypt.com
Product Name	DISK Protect CPA
Version & Platform	8.2.3
Product Description	DISK Protect is an assured full disk encryption solution securing data on touch-screen tablets, laptops, desktops, servers and removable media from theft and loss. Devices can be encrypted at any time and once installed, all data is encrypted transparently, thereby allowing authorized users to access data with no impact on performance. CPA is suitable for organizations that require accreditation (including government, military and NATO organizations), but also available for commercial entities that demand more confidence in their security product. Customers can achieve all the benefits of full centralized management, but would typically be configured for two-factor authentication.

#becrypt

Solution Summary

Becrypt DISK Protect CPA and the RSA Authenticators combine to provide end-users with a single form factor for enterprise-level two-factor authentication. Users can store the necessary keys to unlock the encrypted data on their hard drive on the same device used to provide RSA SecurID authentication throughout the organization.

Partner Integration Overview	
Interoperable through RSA Authentication Client	Yes
Pre-Boot Authentication	Yes
If Pre-Boot, which tokens are supported?	SID800 Rev D4

Product Configuration for Interoperability

Interoperability between the RSA Authenticators and Becrypt DISK Protect CPA requires the installation of the RSA Authentication Client and Becrypt DISK Protect CPA.

Before You Begin

This section provides instructions for integrating RSA Authenticators with Becrypt DISK Protect CPA. The document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

RSA Authenticator Configuration

Before attempting Becrypt DISK Protect CPA installation, please ensure you have properly installed the correct RSA Authenticator drivers. Please consult the appropriate RSA documentation for driver installation details.

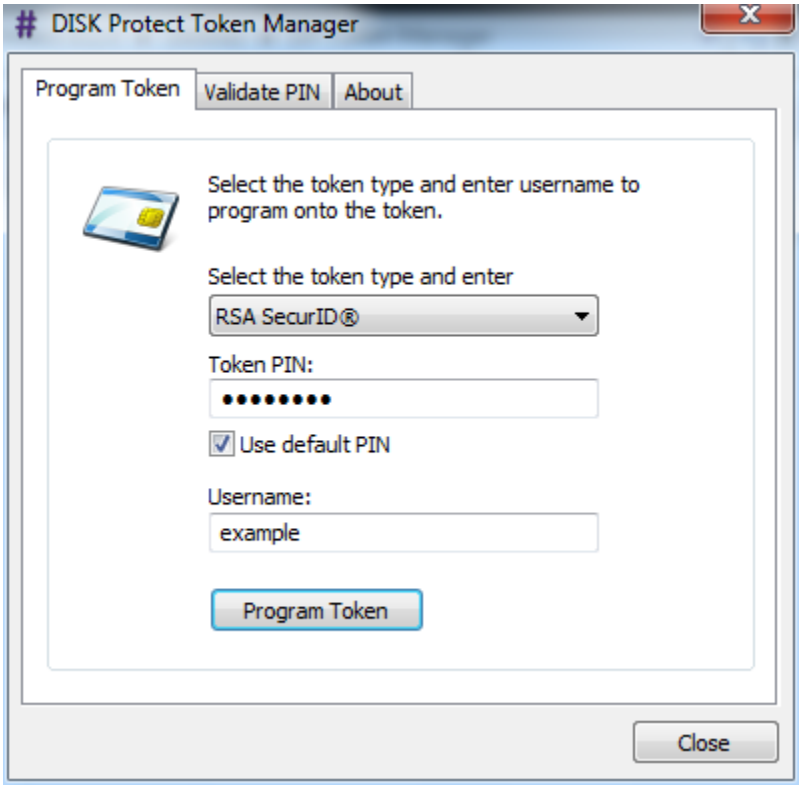
If RSA Security Middleware such as the RSA Authenticator Client is to be used, it can be installed independently of the Becrypt DISK Protect CPA product.

Becrypt DISK CPA Configuration

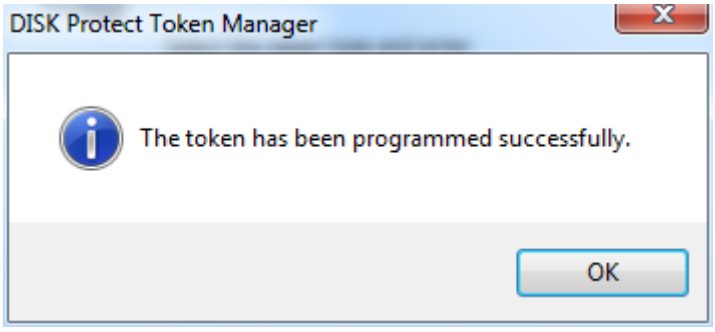
The following instructions outline the procedure for placing the keys on the smartcard and enabling the SID800 at pre-boot. Instructions assume the workstation has RSA middleware installed. Refer to the Becrypt documentation for specific instructions and deployment scenarios.

Program Token with username

1. Launch the Becrypt DISK Protect Token Manager and Select the **token type**. Select **Use default PIN** and **enter** a **Username.** Select **Program Token**.

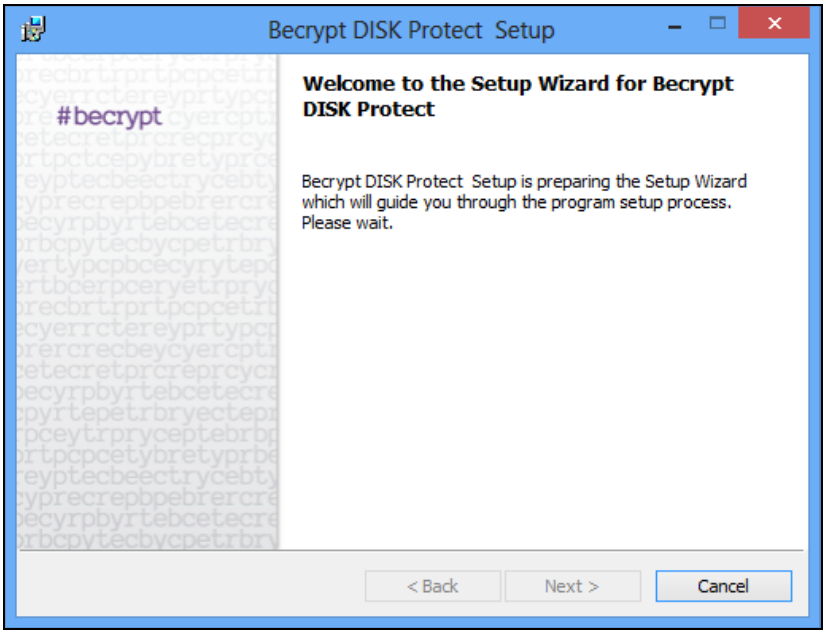


2. Select **OK** to complete the token programming process.

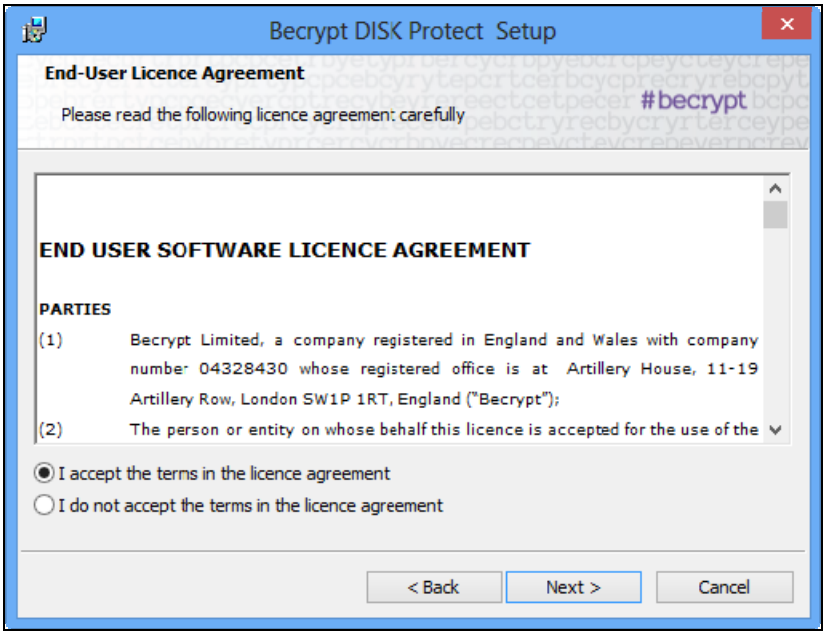


Install Becrypt DISK Protect CPA

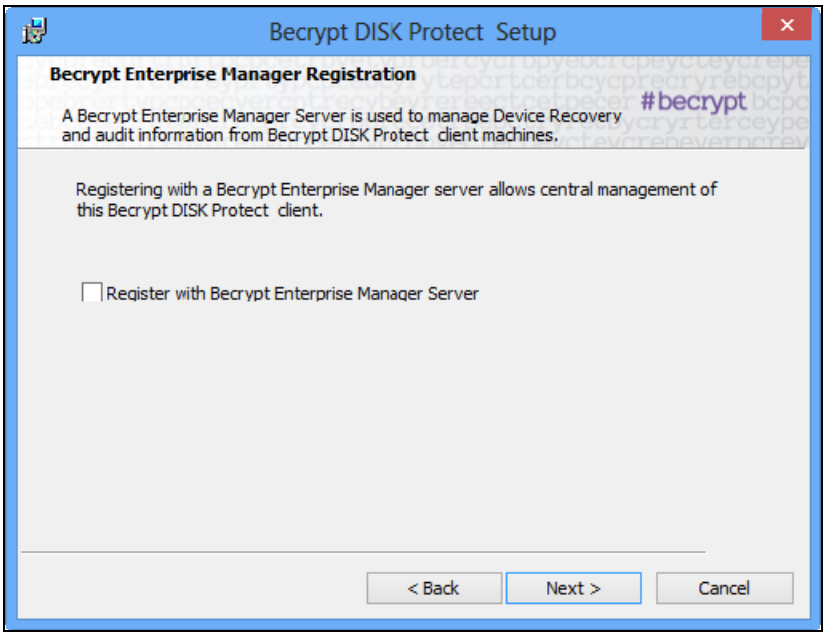
1. Launch the Becrypt DISK Protect CPA MSI and select **Next t**o begin installation.



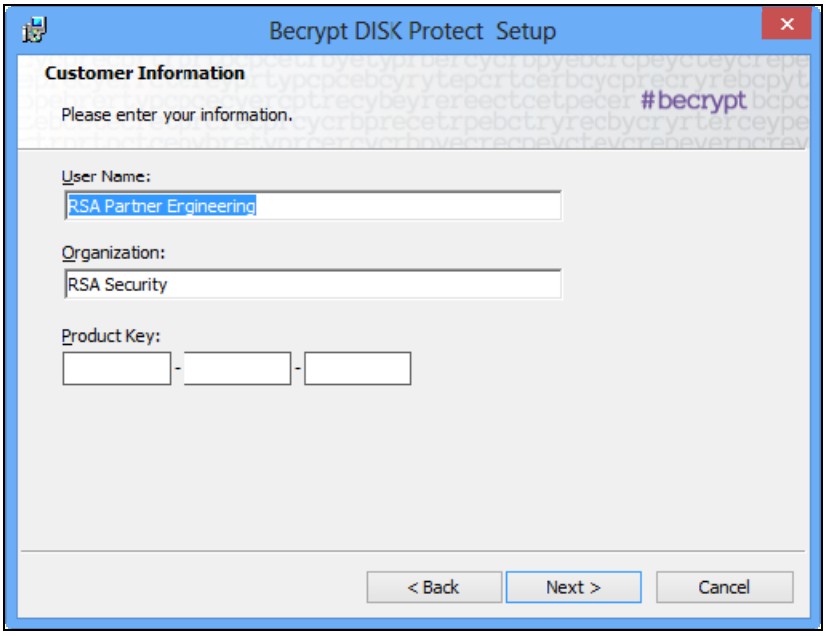
2. Select **Next t**o the End-User License Agreement.



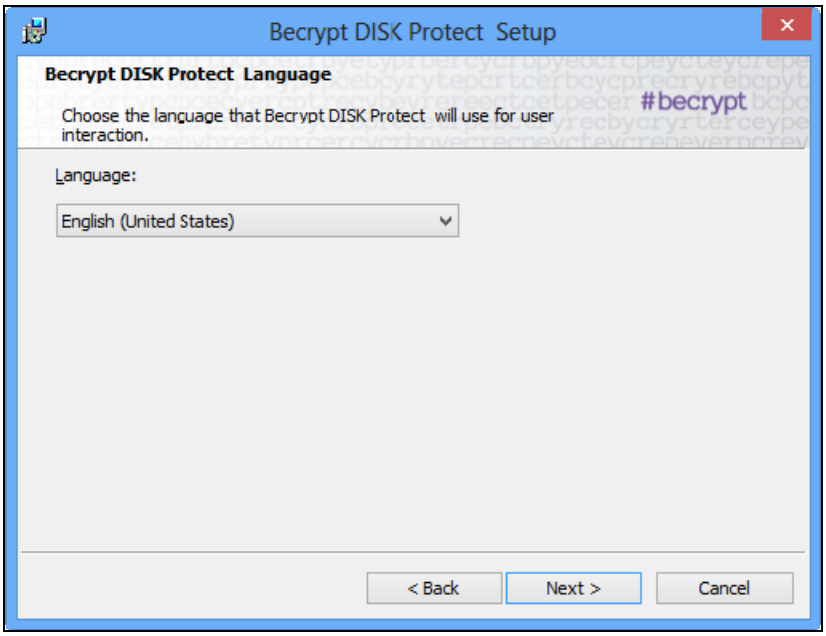
3. Select **Next** to continue with the installation and not register with Becrypt Enterprise Manager Server.



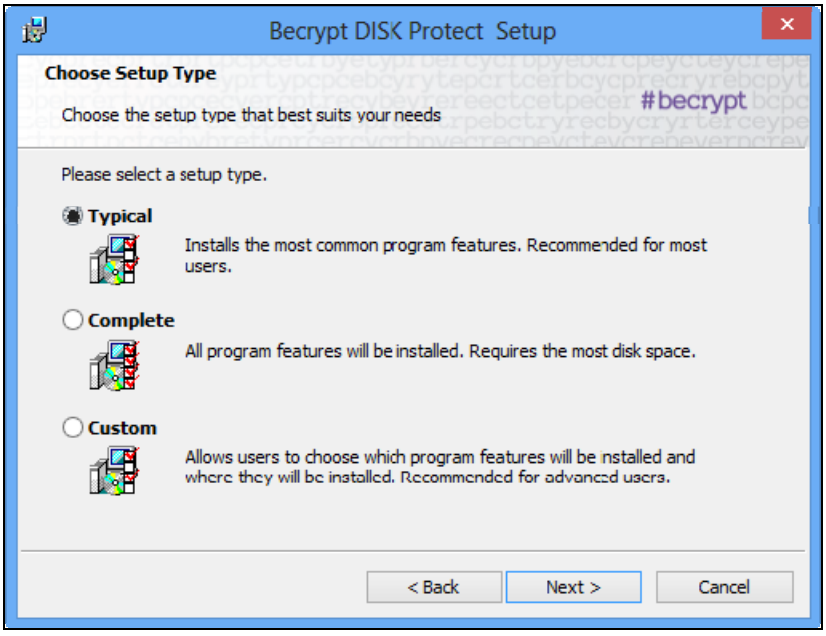
4. Enter a **User Name**, **Organization** to which the product is registered and a valid **Product Key** and select **Next** to continue.



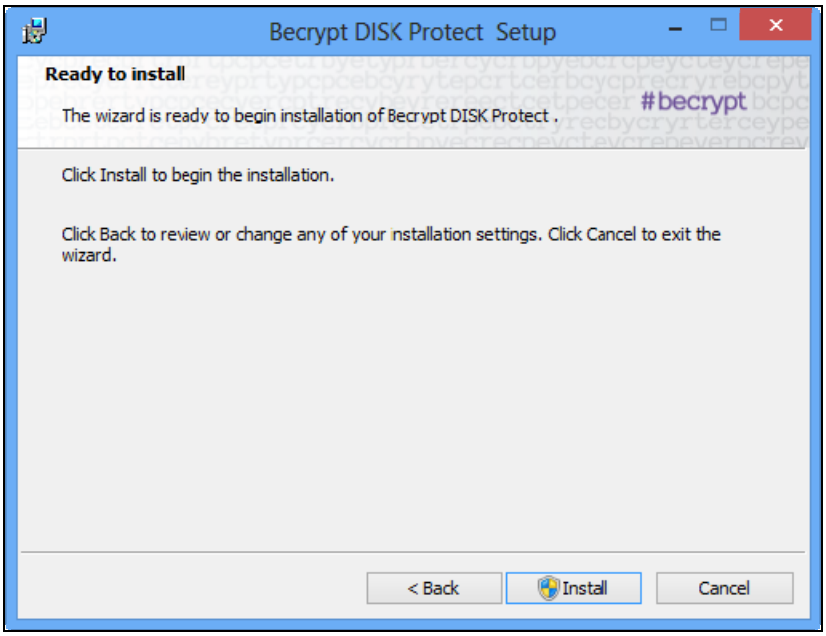
5. Select the **Language** using the drop down for your location and select **Next** to continue.



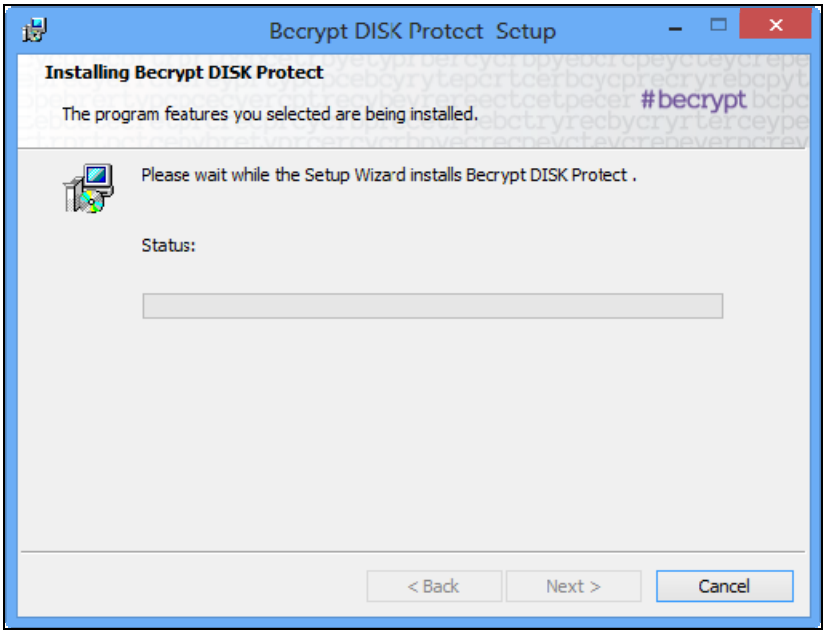
6. Select **Typical** and **Next** to continue.



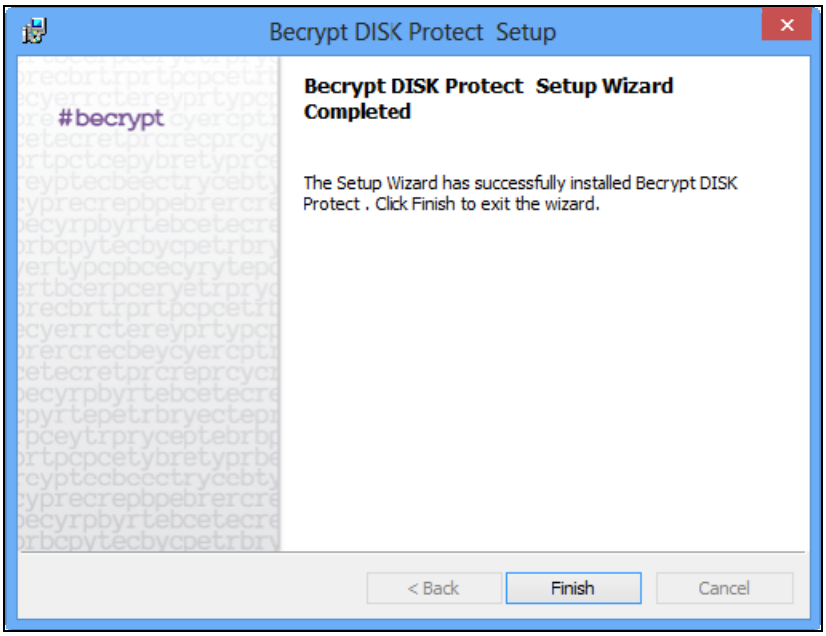
7. Select **Install**.



8. Becrypt will begin the installation process.

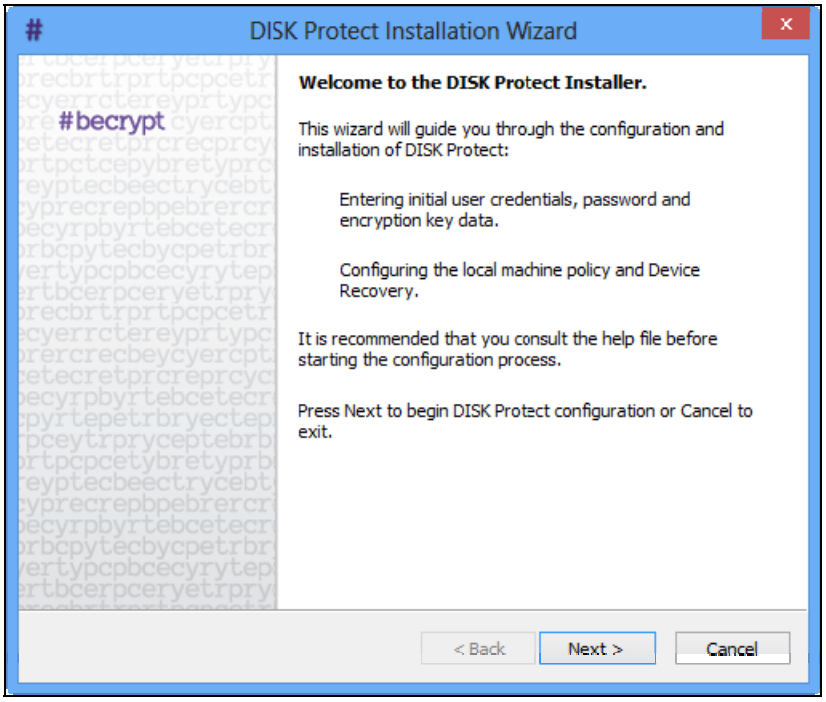


9. Select **Finish** to complete the Becrypt CPA Installation.

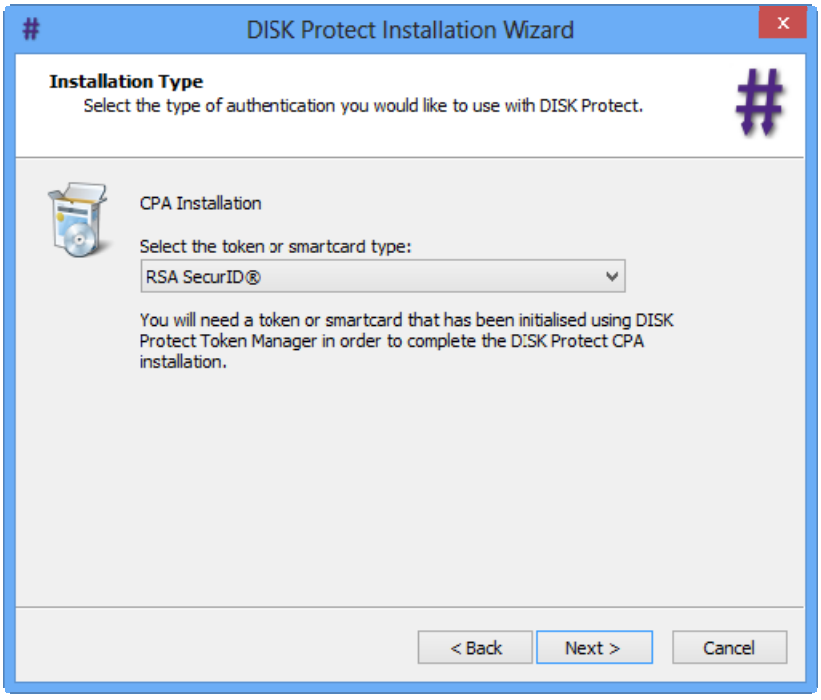


Set the Becrypt CPA Configuration Options

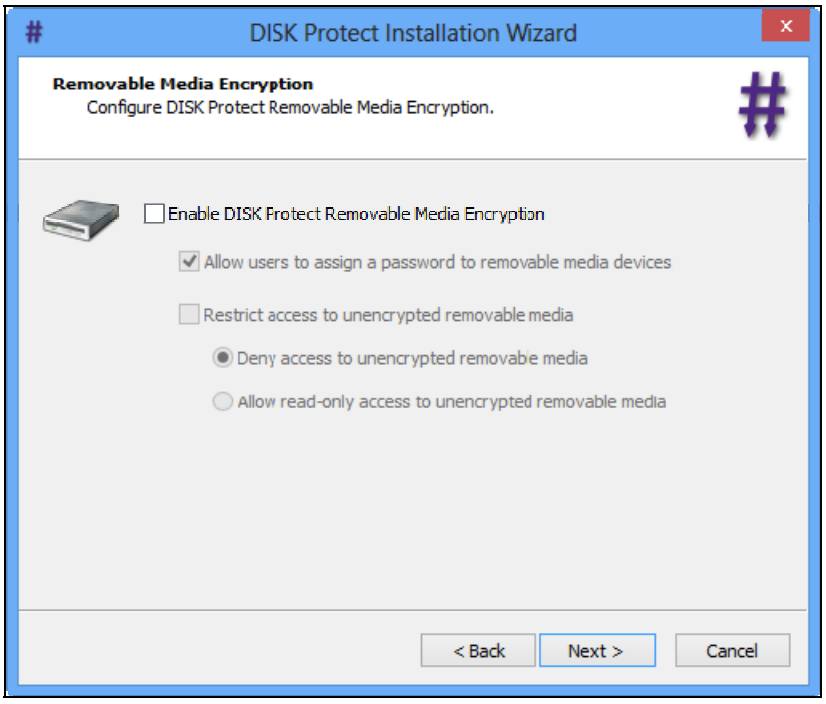
10. Once the MSI has completed the install wizard will start, select **Next** to configure Becrypt CPA.



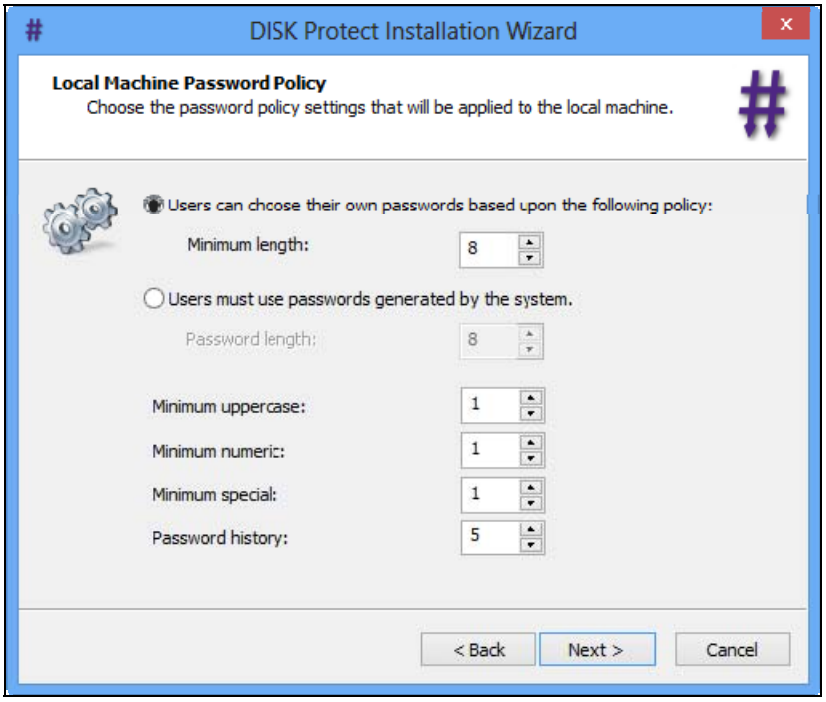
11. Select **RSA SecurID** from the token or smartcard type:



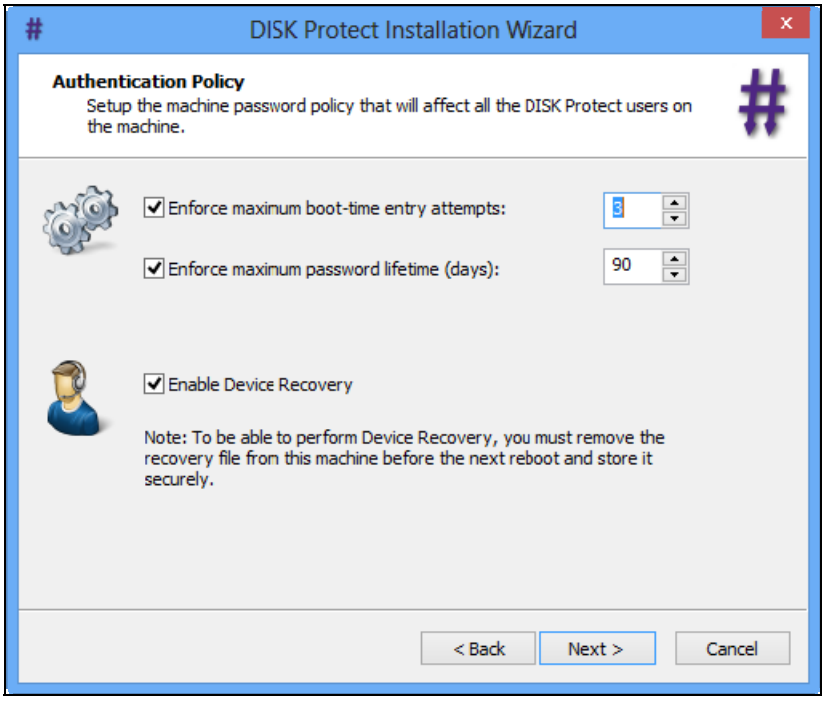
12. Keep the default settings and select **Next** to continue.



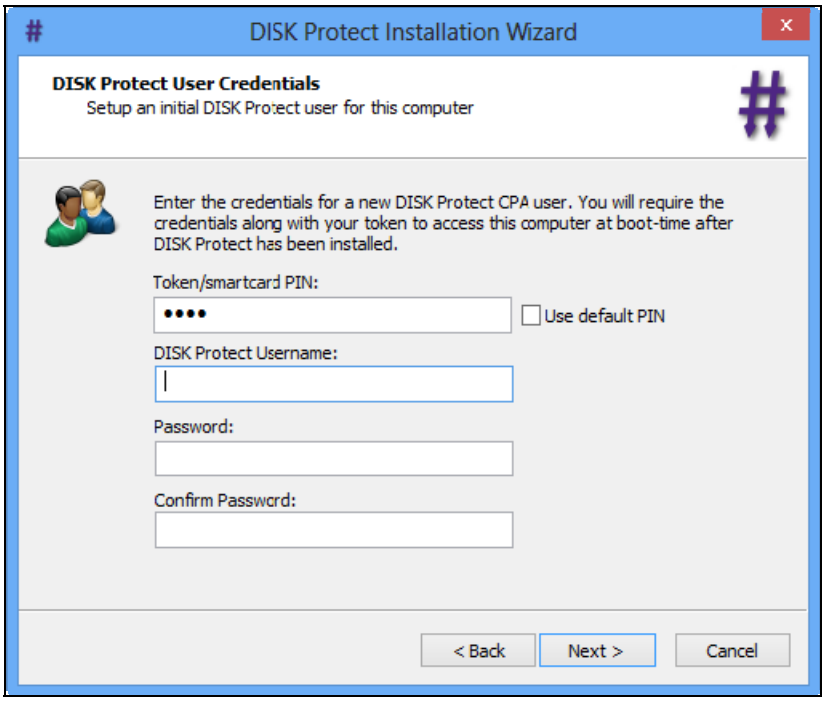
13. Keep the default settings and select **Next** to continue.



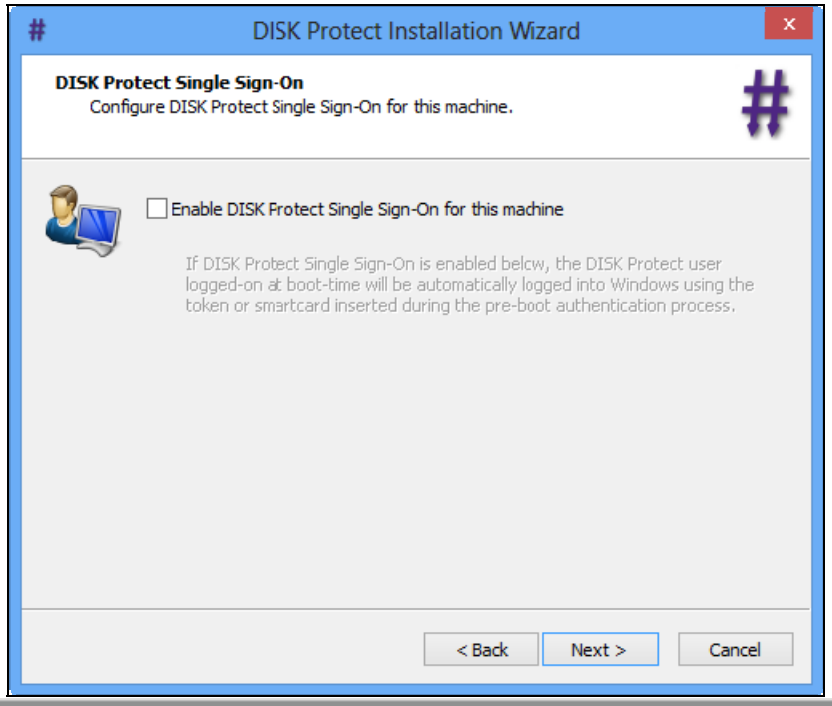
14. Keep the default settings and select **Next** to continue.



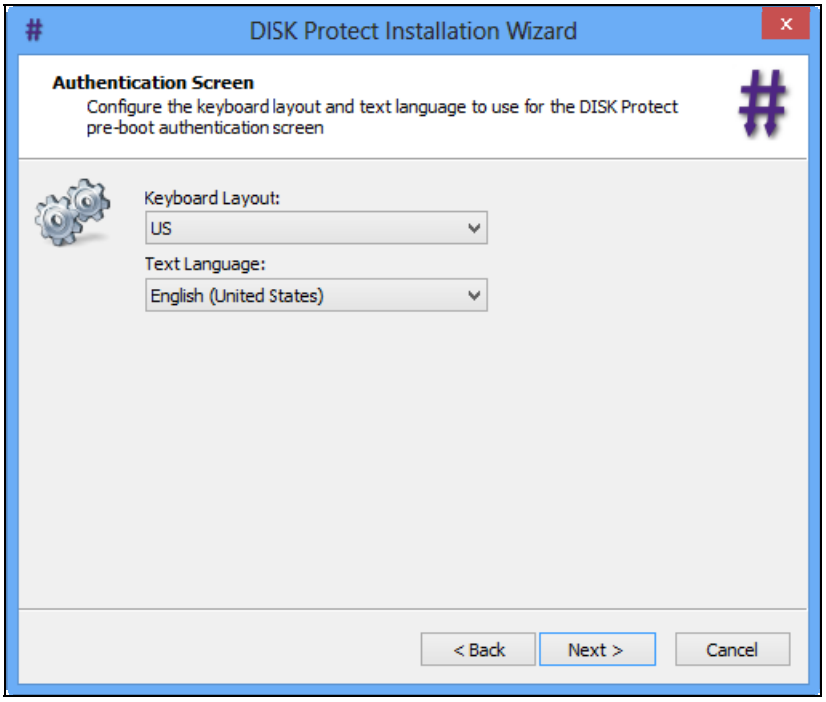
15. Select **Use the default PIN** unless the smart card PIN has been changed from the factory default settings. Enter a **Username**, **Password** and **Password Confirmation**.



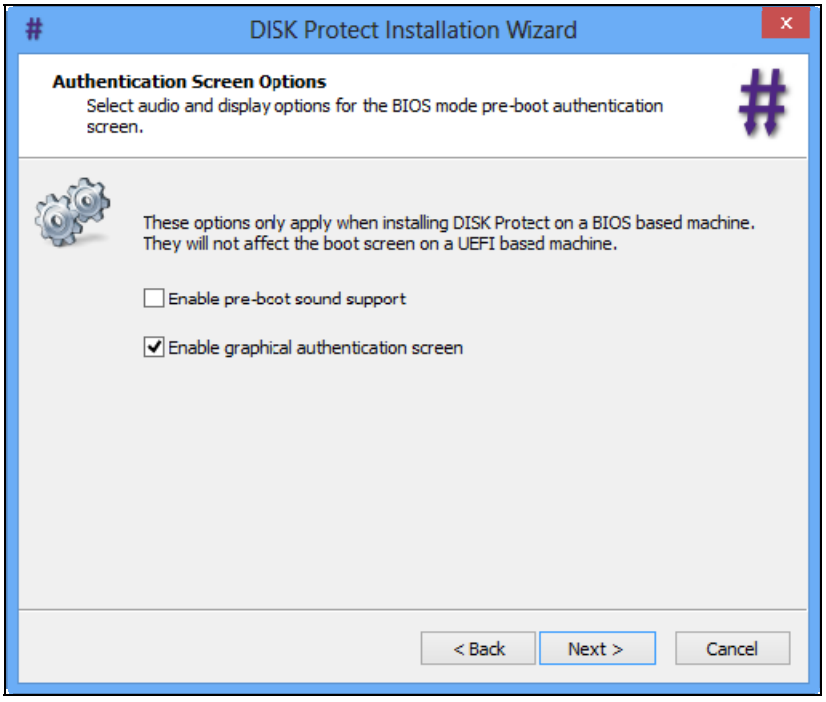
16. Keep the default settings and select **Next** to continue.



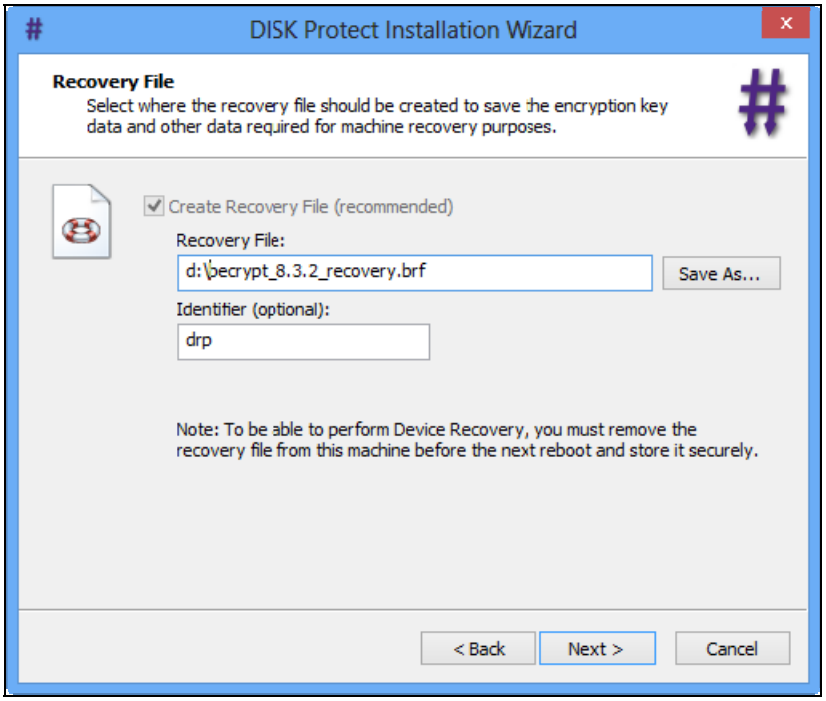
17. Keep the default settings and select **Next** to continue.



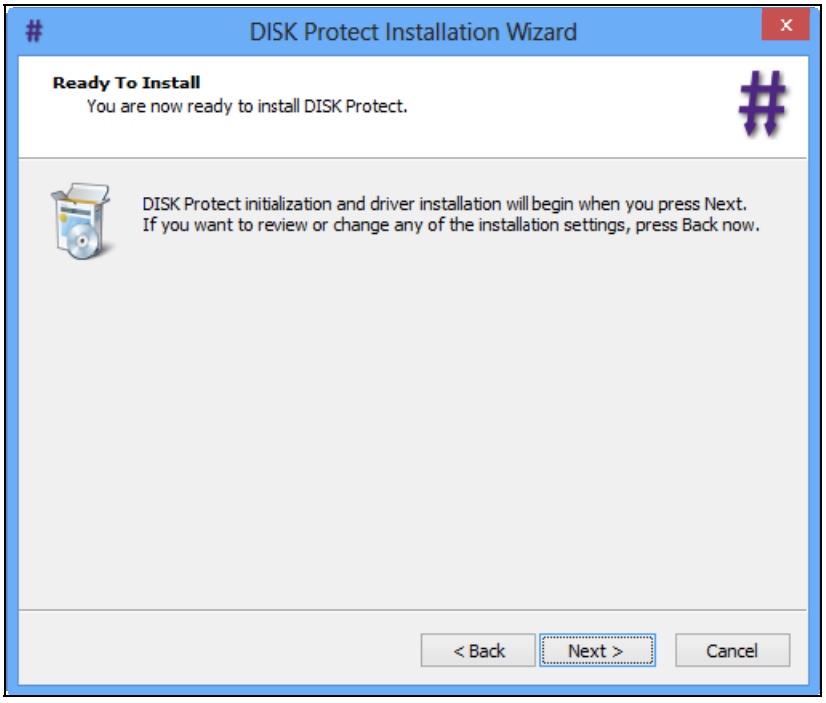
18. Keep the default settings and select **Next** to continue.



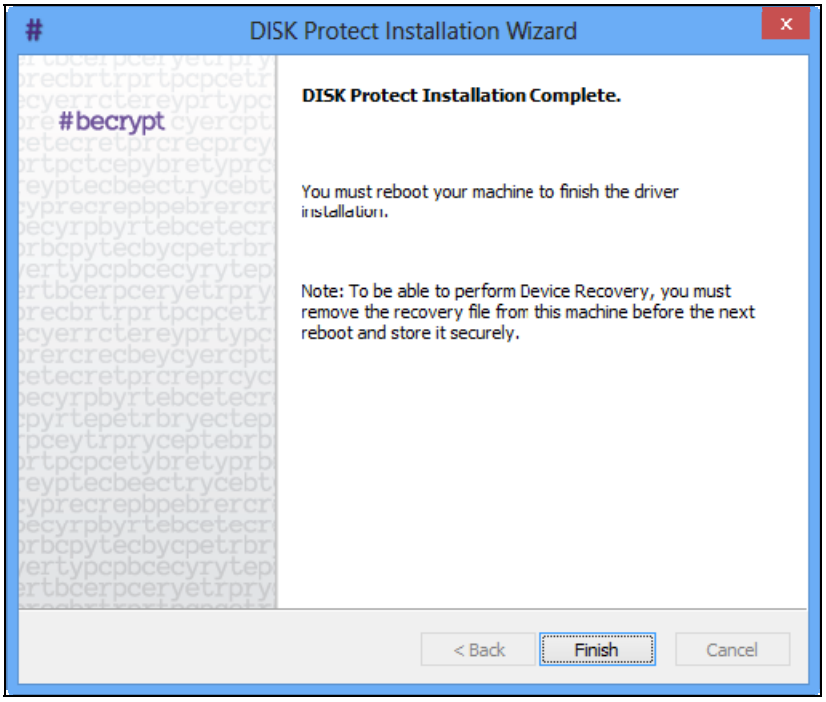
19. Create a Recovery File and **Save t**o a secure location to be used if the user is unable to authenticate with the SID800.



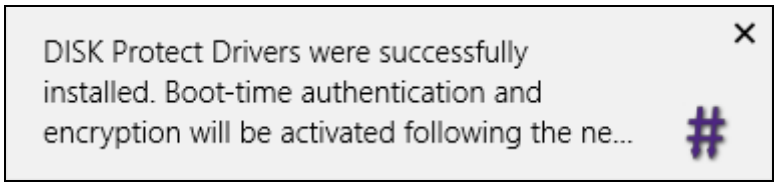
20. Select **Next** to continue.



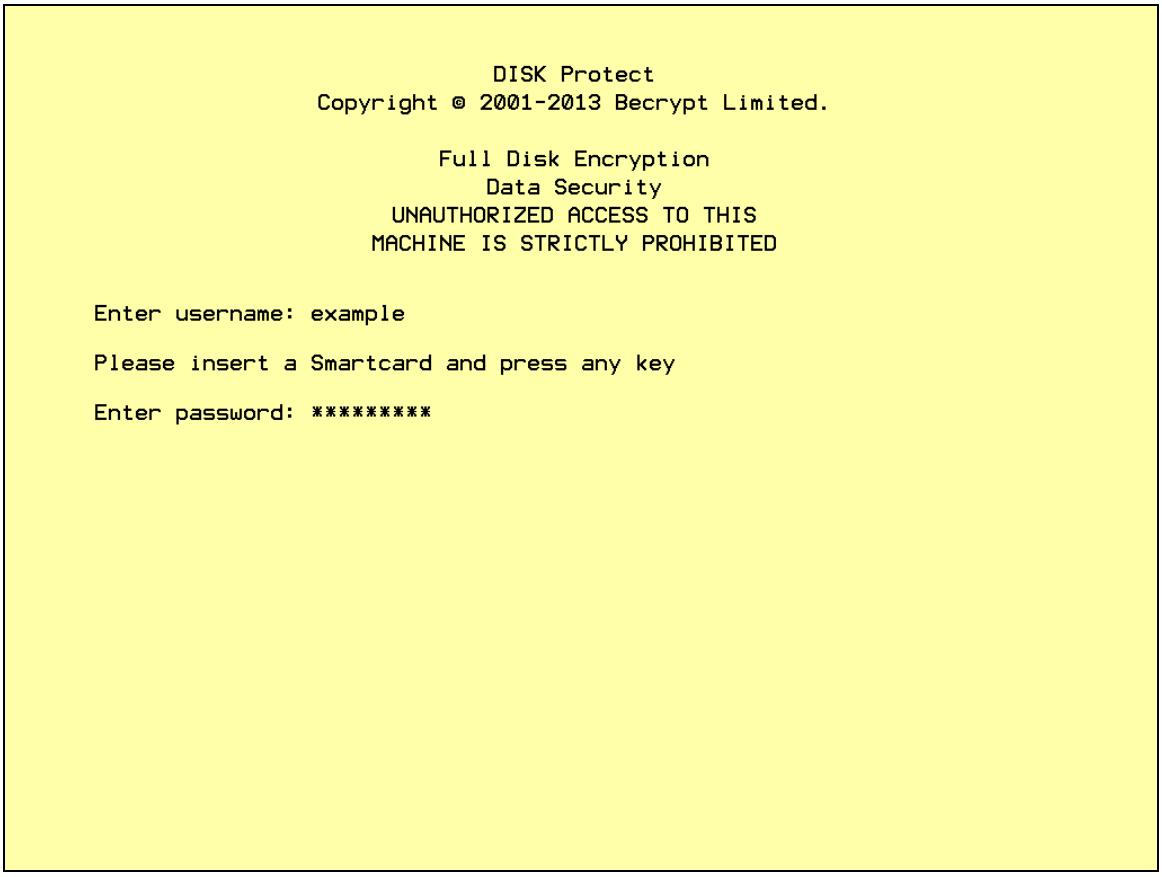
21. Select **Finish t**o reboot the system and continue with the installation of Becrypt CPA.



22. After the OS boots and the user logs in a confirmation of the Becrypt CPA installation will be displayed.



23. At the Becrypt login screen enter the **username**, insert the SID800 smartcard and enter the **password** created in step 15.



Certification Checklist for 3rd Party Applications

Date Tested: December 17, 2014

Product	Tested Version	Operating System
RSA Authentication Client	3.6	Windows 8
Becrypt DISK Protect CPA	8.2.3	Windows 8
RSA SecurID 800	D4	Proprietary

Test Cases	Symmetric Keys	Asymmetric Keys
RSA SecurID 800		
Preboot Authentication	✓	N/A
Disk/File Encryption	✓	N/A
1024 Certificate	N/A	N/A
2048 Certificate	N/A	N/A
Write Key/Certificate	✓	N/A
Delete Key/Certificate	N/A	N/A
Token Management		
RAC API		
Modify Token PIN	N/A	N/A
Verify Token PIN	N/A	N/A
Initialize Token	N/A	N/A

DRP/PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function