



SafeNet Technical Note

ProtectDrive CAC Logon Process

Copyright © 2007 SafeNet, Inc
All rights reserved

This document contains Proprietary and Confidential information of SafeNet, and is protected by copyright, trade secret and other state and federal laws. Its receipt or possession does not convey any rights to reproduce, disclose its contents, or to manufacture, use or sell anything it may describe. Reproduction, disclosure or use without specific written authorization of SafeNet is strictly prohibited.

Generated: 12 Nov 2007 - 11:17

Table of Contents

ProtectDrive CAC Logon Process.....	1
ProtectDrive Disk Encryption Process.....	1
.Key.Description.....	1
Disk Encryption Process.....	1
Pre-boot Smartcard Logon Process.....	2

ProtectDrive CAC Logon Process

Product	Versions
ProtectDrive	8.1 and Later

ProtectDrive provides the ability to authorize access to encrypted laptops using Common Access Cards (CAC). This document describes the process to protect the symmetric disk encryption key and process to authenticate a CAC user to the symmetric disk encryption key.

ProtectDrive Disk Encryption Process

Key Description

Key	Description
UK[uid]	For Certificate Based Logon (CAC Cards, etc): $U_{pub}[uid] / U_{pri}[uid]$ are a user's RSA key pair (RSA 1024/2048) * Each token user has one of these key pairs. * The public key is expected to be available from Active Directory.
	For Username/password based logons: The UK is a user key (AES 256) that is generated from the password-based key derivation function PBKDF2 in PKCS #5 v2.0. * This key is only applicable to password accounts. * Each user password has one of these keys.
DK	The Disk Key (DK) or Volume Key is used to encrypt the system's disk partitions (AES 256). * Each machine with ProtectDrive installed has a unique Disk Key.

Disk Encryption Process

The system is configured to encrypt the hard drives and perform the following functions:

- An AES 256 bit disk key is generated (DK) when pre-boot configuration is activated within ProtectDrive.
- Pre-boot entries are created in the ProtectDrive encrypted file system (EFS) for each authorized user and are managed via Active Directory. A ProtectDrive User account is created for each smart card/token certificate. Including any accounts created for password users, the total number of accounts on each client system can not exceed 2000. ProtectDrive also supports multiple certificates per user as in the case of a user being issued a new CAC card (one entry for old CAC and one for new CAC).
 - ◆ For a certificate user eUK_{pub} (DK)- Disk Key encrypted under the user's public key from user token pub/pri key pair. ProtectDrive utilizes the CAC certificate with Smartcard Logon attributes.
 - ◆ For a password user UK_{pwd} (DK)- Disk Key encrypted under the user's pw based key derivation, PKCS #5 v2.0
- The system encrypts the disks using the generated DK.

ProtectDrive authorizes access to the Disk Key (Volume Key) by storing the following information on the client machine in the EFS:

- eUK_{pub} (DK) - Requires the user's private key to access the DK.
- eUK_{pwd} (DK) - Requires user to provide their password to access the DK.

Pre-boot Smartcard Logon Process

ProtectDrive performs the following steps when performing a Smartcard logon during pre-boot:

- User is presented with pre-boot screen requesting PIN for the CAC card
- ProtectDrive searches the token for certificate with Smartcard logon attribute.
- ProtectDrive then locates the appropriate eUK_{pub} (DK) entry in the EFS
- ProtectDrive decrypts eUK_{pub} (DK) using the user's private key on their smartcard to obtain the DK.
- The system decrypts the disks using the DK allowing access to the operating system.