SafeNet’s strong authentication solutions combine with Becrypt’s DISK Protect to offer full disk encryption and pre-boot authentication as well as secure access to online resources and digital signing.

Becrypt provides a range of market-leading security software to protect enterprise data. Becrypt’s DISK Protect™ provides full disk encryption, strong pre-boot authentication, plus optional removable media encryption, for laptop and desktop computers running Windows operating systems. SafeNet’s eToken PRO is a smart card-based USB authentication token. It offers strong authentication and guaranteed non-repudiation for sensitive applications such as pre-boot authentication and hard disk encryption. eToken’s secure, on-board RSA 1024-bit and 2048-bit key operations enable seamless integration into Public Key Infrastructure (PKI) architectures. eToken can generate and store users’ personal credentials, such as private keys, passwords and digital certificates, inside the protected environment of the smart card chip itself. Users’ private keys never leave the token.

The combination of SafeNet eToken and Becrypt DISK Protect enables users to securely store certificates, passwords and other information required to perform boot-time user authentication and hard disk(s) encryption/decryption.

DISK Protect is a full disk encryption solution for laptop and desktop computers. Together with eToken, DISK Protect provides:

- **Full disk encryption** – DISK Protect transparently encrypts a computer’s hard disk(s), automatically encrypting and decrypting data on the fly so that applications can be used as normal. If an unauthorized user attempts to access the hard drive directly, without going through the User Authentication process, the data remains encrypted and unusable. If the hard drive is later disposed of, any data it contains is unintelligible, even if specialist data recovery tools are used. When DISK Protect is combined with eToken, the encryption keys used to encrypt and decrypt the hard disk(s) data are securely stored on-board the token’s smart card chip. Only successful User Authentication to the smart card chip will allow access to the relevant encryption keys to encrypt/decrypt hard disk data.

- **Boot-time authentication** – Authenticating the user at boot-time means that the operating system may be encrypted to prevent unauthorized data access using low-level tools. When DISK Protect is combined with eToken, the encryption keys that enable the Operating System to be read and booted are securely stored on the token. In order to boot the operating system, the user must successfully authenticate using strong, 2-factor authentication (token plus PIN).
Key SafeNet eToken
**Benefits**
- Paperless office for efficient and cost-effective organizations
- Dual solution for digital signing and secure access based on strong two-factor authentication
- Offer a portable USB design: users carry their digital identity with them - no special reader needed
- Based on industry-standard interfaces for out-of-the-box integration with digital signing applications
- Cost-effective: no back-end infrastructure or ongoing maintenance required

**Features**
- On-board PKI generation; private keys are never exposed outside the hardware token or module for secure storage of user credentials, keys and sensitive information
- FIPS 140-2 validated cards and Common Criteria certified smart card chips
- Native support for long key encryption including RSA 2048-bit

- **Removable media encryption** – DISK Protect encrypts mass storage devices, such as USB memory sticks, to protect data in transit. eToken NG-FLASH is a USB device that combines the high security of a smart card-based USB authentication device with the benefits of flash memory, all in one device. DISK Protect combined with eToken NG-FLASH, enables users to securely store their boot-time credentials and disk encryption keys on board the token’s smart card, and also carry their data on an encrypted/secured flash memory stick.

**Benefits**

**eToken PRO**
- Improves productivity by allowing employees and partners to securely access corporate resources
- Enables compliance with security and privacy standards (FIPS 140-2, Common Criteria certified chip)
- Portable USB design: no special reader needed
- Cost-effective: doesn’t require back-end infrastructure or ongoing maintenance
- Uses extremely portable and flexible USB smart card tokens
- Simple and easy to use – no training or technical know-how needed
- Expand security applications through on-board Java applets
- Enhance marketing and branding initiatives with private labeling and color options

**Becrypt DISK Protect**
- Full disk encryption with encryption keys securely stored on token smart card
- Robust User Authentication process requiring 2-factor authentication (token plus PIN)
- Multi User Capability
- Transparently encrypts a computer’s hard disk(s), automatically encrypting and decrypting data on the fly
- Data remains encrypted and unusable if both token and correct PIN are not present (2-factor authentication)
- Data is encrypted and unintelligible, even if specialist data recovery tools are used
- User credentials and encryption keys are securely stored

**eToken NG-FLASH**
- Enhances productivity by offering secure connectivity to networks, applications, and web-based services
- Offers flexibility by combining strong two-factor authentication with encrypted data on portable eToken NG-FLASH devices
- Reduces costs associated with data loss by protecting valuable business resources and data
- Enables compliance with regulations mandating data security and privacy protection (FIPS 140-2, Common Criteria certified chip)
- Allows full portability of user data – up to 16GB stored in flash memory
- Saves time with auto-run feature that pre-loads applications directly from the token

**Becrypt DISK Protect – Removable Media Encryption**
- User data is portable and secured
- All-in-one device used for (i) authenticating user to DISK Protect, (ii) secure storage of encryption keys and credentials, and (iii) secured and portable mass storage.

**About SafeNet**
Founded in 1983, SafeNet is a global leader in information security. SafeNet protects its customers’ most valuable assets, including identities, transactions, communications, data, and software licensing, throughout the data lifecycle. More than 25,000 customers across both commercial enterprises, and government agencies, and in over 100 countries trust their information security needs to SafeNet.

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com
Follow Us: www.safenet-inc.com/connected

©2012 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners. SB (EN)-10.23.12

eToken™ for Becrypt DISK Protect™ Solution Brief