



Akoura products are designed to increase industry adoption rates for information security through technology innovation and improving the experience of the end-user. Akoura provides enterprise users the strongest possible two or three tier end-user authentication and an industry leading information protection technology. Akoura product suite allows users to protect sensitive information wherever it is stored, and whatever the format.

PrivateDisk Software Solution

Protecting information at rest on a desktop, server, virtual office computer, laptop or other mobile computing device is a critical, growing enterprise security requirement. Akoura's innovative Private Disk product is host-device information protection solution. Private Disk ensures that information stored on any local host can be accessed only by an authorized, authenticated user. The Private Disk cryptographic data store utilizes strong authentication and supports enterprise master key holder.

Private Disk is an ideal solution for any enterprise with a mobile workforce or a critical requirement to protect sensitive or confidential information. Private Disk provides mobile workers a host-device "cryptographic data store" for easy, highly secure information protection. Increasingly mobile workforce and "virtualization" of sensitive and confidential information is a critical security issue for enterprise users. Private Disk ensures that users can store sensitive information on any mobile computing device with the strongest commercially available encryption on the market. To protect a file, a user simply "drags and drops" the file into the cryptographic data store on the desktop.

How PrivateDisk Works

Akoura Private Disk is a host-device only version of Akoura DataSecure. Private Disk leverages the same breakthrough information protection software as DataSecure and provides customers the same unprecedented levels of security. The Private Disk

"cryptographic data store" protects information on a host device through the use of a very large key based encryption and a unique obfuscation technology that digitally "shreds" sensitive information saved within the "cryptographic data store", encrypts and obfuscates the bits, and saves them on the host device drive so they are invisible except to the properly authenticated individual.

Private Disk "cryptographic data store" can reside on a laptop, desktop, network drive, the web, or a removable media. Each "cryptographic data store" provides a catalog of protected files. Access to the "cryptographic data store" is only provided via biometric authentication. Files secured within the data store are unknown to the host-device operating system. Presentation of strong authentication opens the "cryptographic data store" and allows for secure access to the protected information.

Unlike traditional encryption, Private Disk technology protects information in a way that leaves no visual or digital signature. One of the principal benefits of Private Disk is that it ensures a highly secure, anonymous, storage and archival, of sensitive or confidential information.

Unrivaled Benefits

Highly Secure

An innovative combination of encryption, obfuscation technology, and strong authentication provide the highest level of host-device information protection. Protected files leave no visual or digital signature and are almost impossible to detect. The use of biometric authentication eliminates password vulnerabilities.

Reliable: Private Disk is proven, commercially available host-device information protection software. Akoura has partnered with leading strong authentication vendors.

Unprecedented Security: Private Disk protects sensitive information independent of file type or host. Once protected, retrieval is based exclusively on strong authentication.



Easy to Use and Install: Private Disk is a simple host-device software application. Private Disk is simple to use and easy to install and deploy. The total time required to install the software application and complete the fingerprint enrollment process is less than fifteen [15] minutes. Akoura's implementation of "drag and drop" encryption is the simplest method commercially available for protecting information. Implementing Private Disk requires zero incremental network or security infrastructure. Its ease of use makes Private Disk effective in driving increased adoption rates and improving security.

Features and Requirements

PrivateDisk offers the following features:

- Size of data store equals storage available on the host computer / web location
- Industry Leading very large key based Encryption
- Single User or Enterprise Model
- Strong Authentication
- Dynamic Encryption Algorithms
- Symmetric Key Based Encryption
- Drag and Drop Encryption
- OEM Solution

The minimum requirements needed to use PrivateDisk are:

- Windows 2000 or XP
- 256 MB RAM
- 1 GB available disk space
- 1 USB Port
- Microsoft .NET Framework 1.1 or above

Call us at 781-245-3536 to order your software today or go on our website at www.akoura.com to download more information.

About Akoura

Akoura is located in Cleveland, Ohio. Akoura is dedicated to increase industry adoption rates for information security through technology innovation and improving the experience of the end-user and is committed to developing security solutions that offer the strongest levels of commercially available information protection technology, with zero incremental investment in infrastructure, and a simple, functional end-user experience.

Akoura, PrivateDisk, DataSecure and MailSecure are trademarks of Akoura Biometrics, Inc.