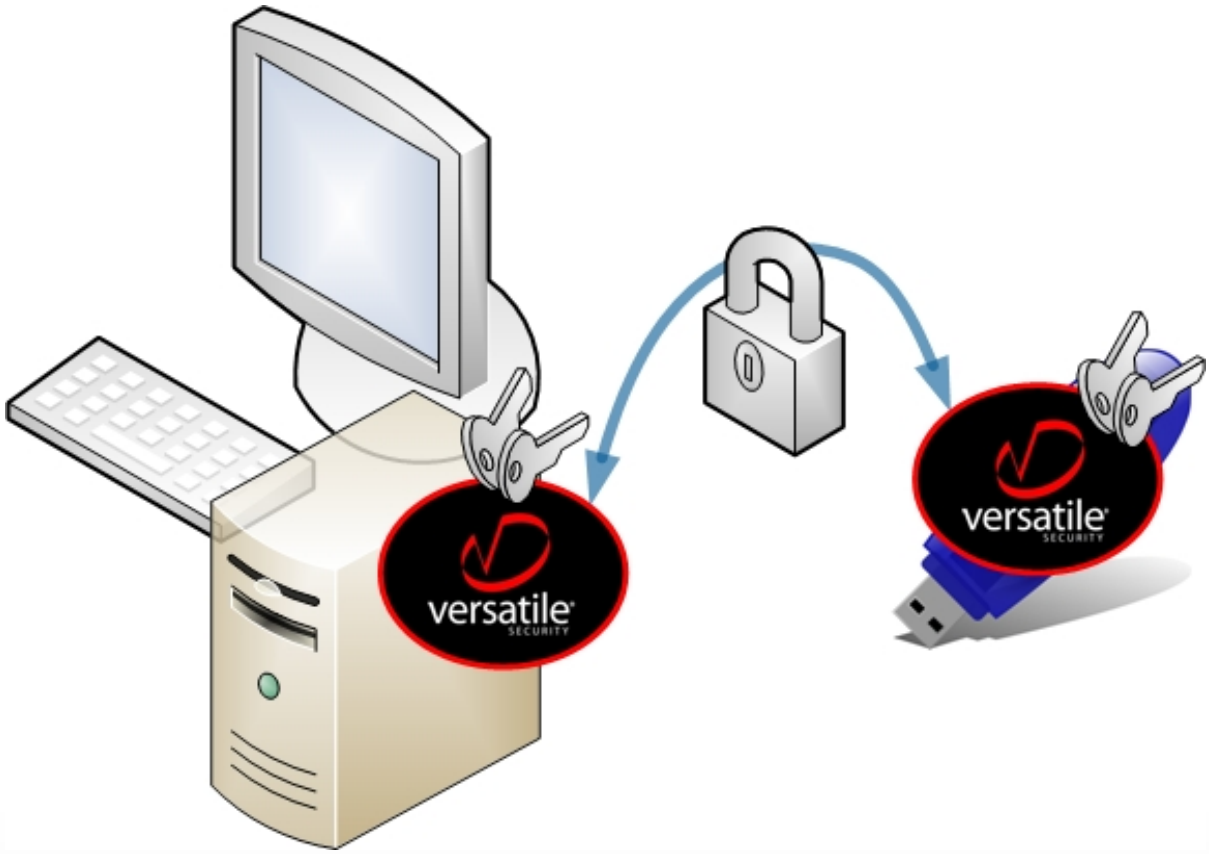
versatile SECURITY

Global Identity Solutions

vSEC:USB Data Access Controller



Data Mobility

Over the years the amount of data created and held has grown enormously. Initially with main frames it was held centrally and the need to transfer was minimal so security was tightly controlled.

With the advent of networks it was possible for users to make copies and backup locally, often leading to security concerns. The amount of data that could be copied was restricted because of the capacity of the media (ex 1.44MB). In order to resolve this, organizations stopped deploying PC's with removable media so that users could no longer make copies.

With the wide availability of USB mass storage devices it is now possible for users to copy large amounts of data in many gigabytes and then restore it on other PC's with no control. The vSEC:USB Data Access Controller allows organizations to implement a trusted policy to ensure their data can only be moved between trusted USB devices and PC's under a policy control.

The controller application is designed to work on the Gemalto Smart Enterprise Guardian (SEG), by utilizing the advantages of the smartcard features of the SEG the application makes it possible to implement a mutual authentication policy, thus ensuring only devices that are trusted as part of the deployment policy can access each other's data stores.

How it works

Using the device is simple. The device is inserted into a USB port. The operating system automatically recognizes the smart card and prompts the user for his/her PIN or pass-phrase. This method of two-factor authentication is more secure than simply entering a user name and password because it relies on something the users have – the SEG and the encrypted identity credentials stored on the smart card, and on something they know – their PIN.

The application can be configured to work within any environment such as a full PKI infrastructure utilizing Trusted Platform Technology (TPM) technology; a background software service on each target device; using a challenge-response mechanism in order to gain emergency access on an unmanaged target device.

The highest level of security can be achieved using TPM technology. TPM is implemented by many hardware vendors. TPMs can be used to authenticate hardware devices. Since each TPM chip has a unique and secret RSA key burned in as it is produced, it is capable of performing platform authentication.

Deployment and policy setting

The management of the vSEC:USB Data Access Controller device and the application is done using vSEC:CMS. The vSEC:CMS Operator Token is a secure, easily integrated and cost effective solution to manage an enterprise's end user smart cards (or other smart card enabled devices such as the Gemalto SEG). The system is delivered on a secure USB token with the application and all settings and credentials' residing securely on the USB token – no installation is required on the target system.

The access control and policy settings provided by vSEC:USB Data Access Controller is granular and role based. Role based access control provides administration advantages in larger systems.

USB Device

The USB device used, the SEG, is natively supported in Windows Vista and Windows Server 2008 and drivers are also available via Windows Update for Windows 2000, XP & Server 2003. This level of integration enables the device to work seamlessly with the entire suite of Microsoft operating systems, software applications and security products. It also makes it simple to deploy and manage of strong authentication and PKI systems without additional software or middleware.

Technical Specifications

Operating Systems

- MS Windows 2000, XP, 2003, Vista, 2008

USB Tokens

- Gemalto Secure Enterprise Guardian (SEG)
- Available with 1 and 2 GB storage capacity

Security features

- Secure key storage
- Role and policy based access control
- Audit log

versatile® SECURITY