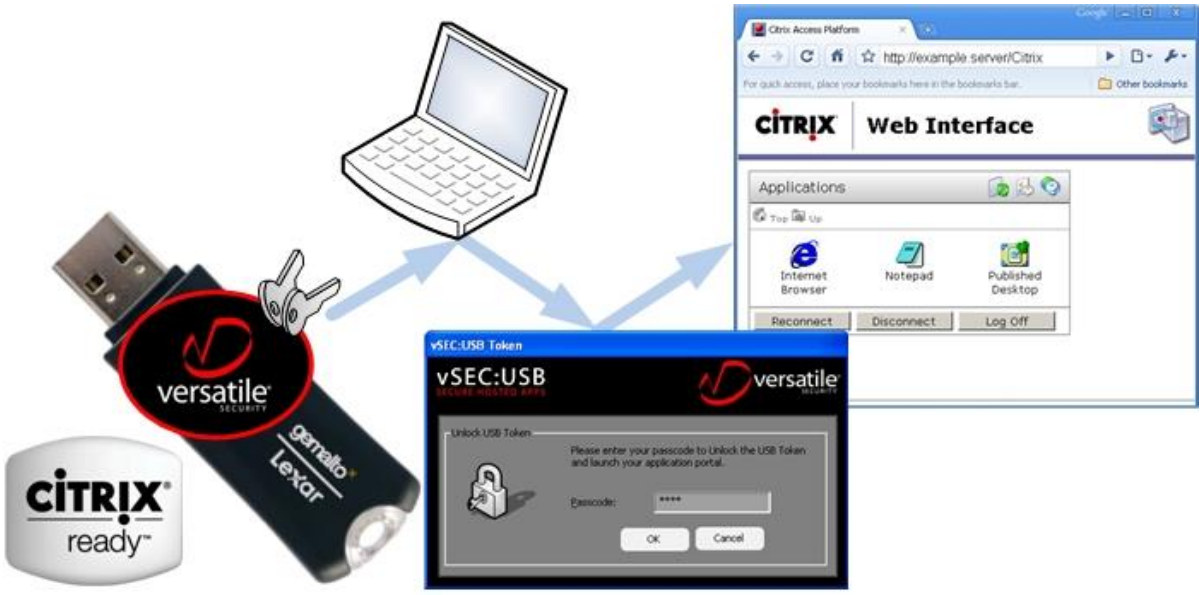
vSEC:USB Secure Hosted Apps



Cloud Computing and Citrix

Citrix is a remote access/application publishing product that allows users to connect to their corporate applications, available from central servers or through a cloud provider as software-as-a-service (SaaS). Citrix lets users connect to these applications remotely, from their homes, airport Internet kiosks, Internet cafes, smart phones, and other devices outside of their corporate networks. From an end-user perspective, users can log in to their corporate network and see all of the applications they would see every day at work, including email and any internal applications. To the user, the application would appear as if it was installed and running on their computer (seamless desktop integration), whereas in reality, the application is running on a server accessible over the Internet - the Cloud.

The Issue

The issue with remote Citrix access is that it is necessary to have Citrix specific client software installed on the device the user is attempting to connect from. It is unlikely that the necessary client software would be installed on the remote device that the user is attempting to connect from.

The Solution

vSEC:USB Secure Hosted Apps is designed to work on the Gemalto Smart Enterprise Guardian (SEG) USB hardware device. vSEC:USB Secure Hosted Apps allows mobile Citrix users to conveniently connect to their corporate applications by simply attaching the SEG to the USB port on the device the user is connecting from. No software needs to be installed on the device the user is connecting from. The operating system on the device automatically recognizes the smart card on the SEG 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. After successfully entering their PIN and authenticating the vSEC:USB Secure Hosted Apps automatically launches the users Citrix web portal using the embedded vSEC:USB Secure Hosted Apps browser giving the user access to their published Citrix corporate applications. On removing the SEG there is no data left on the device the user is connecting from.

Deployment and Management

The management of the vSEC:USB Secure Hosted Apps device and the application is done using vSEC:CMS. The vSEC:CMS T-Series 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.

For more information regarding vSEC:CMS, such as product sheets and demonstrations, visit http://versatilesecurity.com/.

USB Device

The USB device used, the Gemalto Smart Enterprise Guardian (SEG), is natively supported in Windows Vista, 7 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.

The SEG is verified to be compatible with Citrix:

Citrix Product	Version	Operating System
Password Manager	4.0	
Password Manager	4.5	
XenApp	4.0 (Presentation Server)	32-bit
XenApp	4.5 (Presentation Server)	32-bit

Technical Specifications

Operating Systems

- MS Windows 2000, XP, 2003, Vista, 2008 and Win 7.

USB Tokens

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

Main Features

- Two-factor PKI authentication capabilities
- Secure key storage
- Secure token management
- Virus memory scanner
- Firewall detection scanner
- Ease of use

versatile SECURITY