Bolstering Information Security with Virtual Smart Cards

Sophisticated internal and external cybercriminals pose a growing threat to information assets in corporations and government agencies. Access Control models that protect information resources help, but providing adequate security today involves implementing more than just a password.

Password Strength

Password strength is largely irrelevant. While passwords must withstand an automated dictionary attack long enough for the attack to be detected, those types of attacks are yesterday's news. Attackers now prefer highly evolved phishing and social engineering attacks.

Two-Factor Authentication

Two-factor authentication augments "something you know," (typically a user's password), with "something you have," which usually is a physical device in the user's possession, such as a smart card. Smart cards are ideal for security purposes because data stored on the card is not exportable. Smart cards provide a secure operating environment where the cryptographic operations inherent to information security take place. This environment is contained within a processor ("chip") on the card and it is impossible for an attacker to either monitor or manipulate what takes place within that processor.

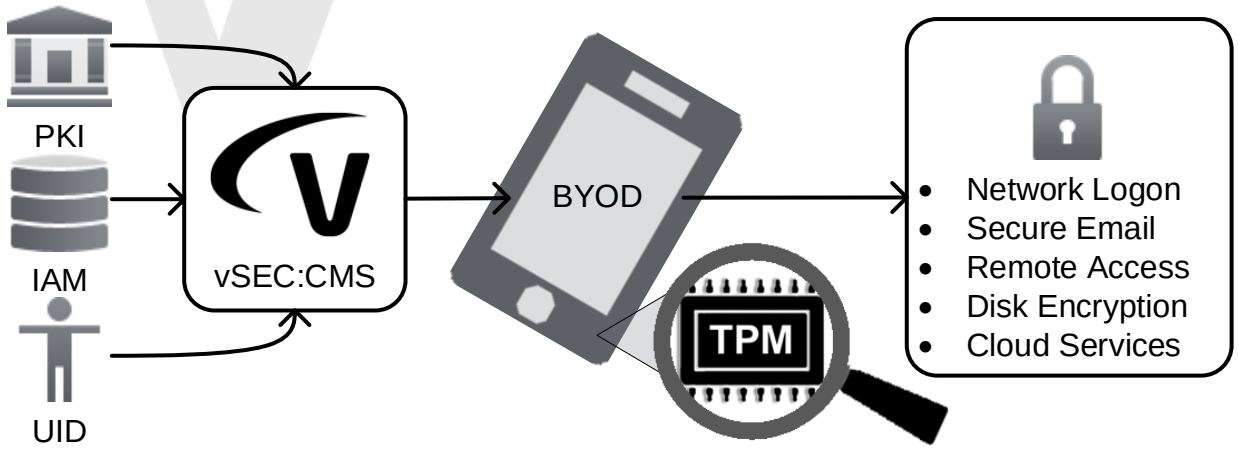
Trusted Platform Module

Most computer manufacturers include a secure processing chip known as the Trusted Platform Module (TPM) on the computer's motherboard. The same cryptographic operations that take place in a smart card also take place in the TPM. As with a smart card, cryptographic keys can be securely stored in the TPM.

Enter the Virtual Smart Card

With Windows 8, Microsoft introduced the concept of Virtual Smart Cards that emulate smart cards in a virtual sense by making use of the TPM. Using vSEC:CMS from Versasec, it is possible to create and manage the lifecycle of a virtual smart card leveraging the Microsoft implementation.

Versasec's specialized software emulates and manages virtual smart cards using the TPM through vSEC:CMS effectively serving as a virtual smart card. In effect, the Versasec software program serves as a virtual smart card. While the software interfaces with both operating systems and application programs as would a physical card, it also refers processing of cryptographic commands and cryptographic key storage to the host computer's TPM. The benefit of this approach is that organizations deploying the vSEC:CMS Virtual Smart Card technology need not purchase smart cards or smart card readers, resulting in reduced overall solution costs without compromising security. With Versasec's implementation, users can create and manage Virtual Smart Cards from Windows 7 and above. Microsoft's implementation is supported from Windows 8 and above.



Lifecycle Management of Virtual Smart Card

Versasec's vSEC:CMS streamlines and simplifies Virtual Smart Card Lifecycle Management

- Installs in minutes, rather than weeks or months for similar solutions
- Requires no dedicated hardware or servers
- Employs a self-service capability that simplifies deployment
- Offers a low total cost of ownership with no hidden costs
- Provides consistently high levels of security, without exception
- Supports management of TPM-enabled devices from Windows 7 and above
- Full management capabilities of Virtual Smart Cards for Microsoft Windows 8 and above.

Remote Service Device Management (RSDM)

For remotely managing the Virtual Smart Cards on their users' devices, customers can use the RSDM in conjunction with Versasec: User Self Service (vSEC:USS). Using this allows the administrators of vSEC:CMS S-Series to centrally manage Virtual Smart Cards on any user's device, regardless of the device's location.

Example: Temporary Credential

Consider the scenario where a remote employee uses a laptop with an embedded TPM and a conventional smart card token to securely access the corporate network via VPN. If the employee loses her smart card token and cannot access the corporate network, what are her options? The answer is simple using vSEC:CMS.

1. Call the IT helpdesk; request a temporary card.
2. After performing security clearances with the employee, the helpdesk worker enables the Virtual Smart Card template on the vSEC:CMS. The helpdesk worker also revokes the employee's conventional smart card, rendering it obsolete.
3. The employee launches the vSEC:CMS User Self-Service application on her laptop and, using the wizard-driven process, a Virtual Smart Card will be created and issued with a time-limited VPN certificate credential.
4. The employee can now log onto the VPN with two-factor authentication and access the corporate network.
5. When the remote employee receives her new conventional smart card token, she can activate it using the vSEC:CMS User Self-Service application. Once the smart card token is activated, the VPN certificate credential on the Virtual Smart Card is automatically revoked.

Example: BYOD

Corporations increasingly rely on Bring Your Own Device (BYOD) policies, which challenges IT departments in ensuring these disparate devices are provisioned with strong credentials. Devices embedded with a TPM can be managed with vSEC:CMS.

1. An employee wishes to use his Windows tablet with an embedded TPM for corporate network access.
2. A vSEC:CMS operator creates a Windows tablet template in vSEC:CMS, which creates a Virtual Smart Card and issues a network logon certificate credential.
3. Using the wizard-driven processes in the vSEC:CMS User Self-Service application which is installed on his Windows tablet, the employee can create and issue the network logon certificate credential to his device.
4. The employee can now use his Windows tablet to perform two-factor authentication to log onto the corporate network.

"Versasec's Virtual Smart Card management capabilities offer more value to customers who need strong identity protection across the organization. This frees employees from complex and difficult-to-remember passwords, and enables a single sign-on experience on BYOD Windows devices." -- Arnaud Jumelet, Cloud & Security Consultant, Microsoft France.