Today’s organizations, both large and small, are faced with the challenging task of securing a seemingly borderless domain of company assets. Identity and Access Management (IAM) becomes a critical aspect of managing access to company assets, with users connecting from multiple mobile and fixed devices. Security breaches are happening on a daily basis, with millions of usernames, passwords, and associated personally identifiable information being harvested. This information, while valuable in and of itself, is further used by threat actors to impersonate the affected individuals elsewhere, such as on shopping or banking sites. Multi-factor authentication is a critical element to help thwart these ongoing breaches.

**Passwords Aren’t Helping**

Users and organizations often still view their usernames and passwords with a false sense of security. Phishing schemes are becoming more elaborate and often more refined and targeted, with the compromised accounts allowing access to the network where additional identities can be gathered, and new accounts created. While company IT departments enforce password complexity rules and frequent change requirements, users can duplicate or re-use those same passwords on public sites where the security is often less stringent - thus providing another method of compromise. With the advent of cloud computing, processing power is readily available online to assist in brute force attacks to break passwords as well.
Multi-factor Authentication

Multi-factor authentication can take many different forms, and provides a significantly higher level of protection than the standard password approach. Multi-factor authentication is two or more of “Something You Know,” “Something You Have,” and “Something You Are.” A username /password alone is an example of “Something You Know,” and is one dimensional. Smart cards, security tokens, and one-time passwords (OTP) are examples of adding “Something You Have” as a second factor, requiring any account breach to successfully compromise both features before gaining access. Since the second factor is in your possession, it makes it significantly more difficult to breach the account. Smart cards have historically had a large user base in the government and large corporations, providing a reliable two-factor authentication mechanism, but at a high cost.

Traditional Smart Cards

Smart cards are physical authentication devices, which improve on the concept of a password by requiring that users actually have their smart card device (“Something You Have”) with them to access the system, in addition to knowing the PIN (“Something You Know”), which provides access to the smart card. Smart cards have three properties that help maintain their security:

Non-exportability: Information stored on the card, such as the user’s private keys, cannot be extracted from the device and used in another medium.

Isolated cryptography: Any cryptographic operations related to the card (such as secure encryption and decryption of data) happen directly in a crypto processor on the card, so malicious software on the host computer cannot observe or manipulate the transactions.

Anti-hammering: To prevent brute-force access to the card, a set number of consecutive unsuccessful PIN entry attempts will cause the card to block itself until administrative action is taken.
Smart cards provide greatly enhanced security over passwords, as it is much more difficult for an unauthorized individual to gain and maintain access to a system. Most importantly, access to a smart card-protected system requires that users have both a valid card and know the PIN that provides access to that card. It is extremely difficult for a thief to acquire both of these things. This is known as two-factor authentication, or two-factor auth. Further security is achieved by the singular nature of the card: since only one copy of the card and its contents exists, only one individual can use his or her logon credentials at a time and the user will quickly notice if the card has been lost or stolen. This greatly reduces the risk window of credential theft when compared to passwords. Unfortunately, this additional security comes with added material and support costs. Traditional smart cards are expensive to purchase (both cards and readers must be supplied to employees), and they can also be easily forgotten, broken, misplaced, stolen or otherwise not available for authentication. The subsequent revocation and replacement of these tokens is even more expensive on a per token basis than the original deployment. The operational cost and management level has often proven to be an implementation barrier to many organizations.

The TPM, or Trusted Platform Module, has many of the same capabilities as a physical smart card. The Trusted Computing Group (TCG), an industry standards consortium comprised of leading technology corporations, developed the standards for the TPM. The TPM has been part of virtually every business-class laptop and desktop shipped in the last seven years, so it is typically already on the computers used by enterprises. The TPM is an embedded security processor that provides tamper-proof security and crypto functions to the operating system and applications. It provides functionality of RSA key generator and cryptography, message digest generator, HMAC (Hashed Message Authentication Code), Random Number Generator (RNG), Protected Flash, NVRAM and ROM memories, and modules (counters and supply voltage measurement) used for tamper detection. The three primary functions of a physical smart card (non-exportability, isolated cryptography, and anti-hammering) are all features and are supported by the TPM.
Enter the Virtual Smart Card

While the core TPM hardware technology that enables strong authentication and use as a virtual smart card (VSC) has been in existence for some time, the business focus around strong authentication and heightened security are relatively new. One of the key dynamics that enables the use of virtual smart card and makes it accessible to a much wider audience than physical smart card is the elimination of upfront hardware costs as well as ongoing maintenance costs.

In a traditional smart card scenario, a company that wants to deploy the technology will need to purchase both smart cards and (devices with) smart card readers for all employees. Though relatively inexpensive options for smart cards can be found, those that ensure the three key properties of smart card security (most notably non-exportability) are more expensive. TPM virtual smart cards, however, can be deployed with no additional material cost, as long as employees have computers with built-in TPMs; and these machines are extremely common in the market.

Additionally, the maintenance cost of virtual smart cards is reduced over that of the conventional option. Where traditional smart cards are easily lost, stolen, or broken from normal wear and tear, TPM virtual smart cards are only lost or broken if the host machine is lost or broken, which in most cases is much less frequently. Given the many cost factors listed above for physical smart cards and their absence from a virtual smart card cost model, the VSC is typically less than 50% the cost of a physical smart card model while providing the security and strong authentication an enterprise organization requires.

Where can I use a VSC?

The rule of thumb is anywhere you can use a physical smart card, you can use a virtual smart card since they provide the same functions and use the same smart card operating system driver. Virtual smart cards can not only be used for Windows Smartcard Logon, they can also be used for other applications such as Microsoft DirectAccess, VPN, Microsoft Office 365, Terminal Services, 802.1x network access control (NAC), Wi-Fi authentication, and many more. When the security provided by the TPM is paired with certificate-based access to these primary business functions, it is readily apparent that this approach provides a significantly higher security posture for the workstation or virtual terminal.
Deployment is Simple

VSC deployment is a relatively simple process. Wave is currently distributing Wave Virtual Smart Card 2.0, which provides enterprise tools for deployment as well as ongoing lifecycle management of the VSCs.

The card lifecycle can be segmented into three distinct areas:

<table>
<thead>
<tr>
<th>Area</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation</td>
<td>• The deployment of Wave Virtual Smart Card 2.0 can be fully automated through the associated management console (ERAS), domain policies, and the organization’s software distribution system.</td>
</tr>
</tbody>
</table>
| User Login | • Once the VSC has been created, the user logs into this account using standard Windows authentication  
• If certificate auto-enrollment has been configured, the user will be prompted to enroll a VSC certificate where they will need to enter their PIN  
• If auto-enrollment has not been configured, they will enroll their certificate through the standard procedure dictated by the organization  
• The certificate’s key is created within the TPM and is non-exportable |
| Using the VSC | • The user can also easily change their PIN by using the Ctrl + Alt + Del input and selecting Change Password -> Other Credentials  
• After a VSC has been successfully created, it can be used for authentication to a number of programs and applications such as VPN, 802.1x and RDP  
• If there are too many failed PIN entry attempts, the user will be locked out of their card and presented with a challenge code which they would use to call the helpdesk. After providing this code, the IT staff will be able to give them a response code which they can input and use to change their PIN to regain access to their card.  
• Wave VSC management provides centralized management and recovery – it has a built-in challenge-response recovery mechanism that is also available when the user’s computer is off-line (e.g. forgotten password of a VPN certificate) |
A sample enterprise scenario begins with the deployment team determining initial use and rollout schedule. In this case, they have determined that they will use VSC for Windows Logon, DirectAccess, and Office 365 access. Using Wave’s EMBASSY Remote Administration Server (ERAS) Management Console and VSC Deployment Tool, the agent software is deployed to the target machines. By using a certificate authority, system and user certificates are added to the certificate store, and additional capabilities are added as needed (e.g. Virtual Desktop) during the IT lifecycle.

Using the automated deployment tools available, IT departments can rapidly deploy and manage virtual smart cards for their users across the enterprise. Security is enhanced through the use of certificates for authentication. More importantly, organizations moving away from passwords now have the added, critical benefit of all cryptographic processing occurring in the TPM physical device which is far less susceptible to breach and tampering. The main security commands are not executed in the operating system or the main CPU, which can be compromised.
Summary

Virtual smart cards provide equal security to proven physical smart card security schemes, utilizing certificates to implement strong two-factor authentication. By using the Trusted Platform Module (TPM) that is already built in to over 550 million devices in the field, an organization starts with a silicon root of trust that can be extended with further use cases. VSCs and their associated certificates are flexible enough to address not only logon but also application-specific security, integrating with existing PKI schemes. Inclusion of virtual smart cards into a comprehensive security regime will significantly enhance your organizational security posture at a fraction of the cost of other alternatives.

For more information, contact your Wave representative or call (877) 228-WAVE.