Understanding and Evaluating Virtual Smart Cards

*Version 1.2*

**Copyright information**

This document is provided “as-is”. Information and views expressed in this document, including URL and other Internet website references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2015 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, BitLocker, Internet Explorer, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Contents

[1 Introduction 1](#_Toc434486808)

[1.1 Purpose 1](#_Toc434486809)

[1.1.1 Overview 1](#_Toc434486810)

[1.1.2 Audience 1](#_Toc434486811)

[1.2 Options for authentication 1](#_Toc434486812)

[1.2.1 Passwords 1](#_Toc434486813)

[1.2.2 One-time passwords (OTPs) 1](#_Toc434486814)

[1.2.3 Smart cards 2](#_Toc434486815)

[1.3 Virtual smart cards as an option 2](#_Toc434486816)

[2 Comparing virtual smart cards with conventional smart cards 4](#_Toc434486817)

[2.1 Technical 4](#_Toc434486818)

[2.2 Functional 4](#_Toc434486819)

[2.3 Security 5](#_Toc434486820)

[2.4 Cost 6](#_Toc434486821)

[2.5 Smart card vs. virtual smart card summary 6](#_Toc434486822)

[3 Lab setup 8](#_Toc434486823)

[3.1 Goal 8](#_Toc434486824)

[3.2 Prerequisites 8](#_Toc434486825)

[3.3 Step one: Create the certificate template 8](#_Toc434486826)

[3.4 Step two: Create the TPM virtual smart card 12](#_Toc434486827)

[3.5 Step three: Enroll for the certificate on the TPM VSC 14](#_Toc434486828)

[4 Virtual smart card use 16](#_Toc434486829)

[4.1 Version of TPM supported 16](#_Toc434486830)

[4.2 Using Tpmvscmgr.exe 16](#_Toc434486831)

[4.3 Programmatic management of virtual smart cards 17](#_Toc434486832)

[4.4 Distinguishing TPM virtual smart card from physical smart cards 18](#_Toc434486833)

[4.5 Number of virtual smart cards on a computer 18](#_Toc434486834)

[4.6 Number of certificates on a virtual smart card 19](#_Toc434486835)

[4.7 PIN, PUK, and admin key requirements 19](#_Toc434486836)

[4.8 Changing the PIN 19](#_Toc434486837)

[4.9 Authentication 19](#_Toc434486838)

[4.9.1 Use case: Two-factor auth‒based remote access 19](#_Toc434486839)

[4.9.2 Use case: Client authentication 19](#_Toc434486840)

[4.9.3 Use case: Virtual smart card redirection for remote desktop connections 20](#_Toc434486841)

[4.9.4 Windows To Go and virtual smart cards 20](#_Toc434486842)

[4.10 Confidentiality 20](#_Toc434486843)

[4.10.1 Use case: S/MIME email encryption 20](#_Toc434486844)

[4.10.2 Use case: BitLocker for data volumes 20](#_Toc434486845)

[4.11 Integrity 21](#_Toc434486846)

[4.11.1 Use case: Signing data 21](#_Toc434486847)

[5 Deployment of virtual smart cards 22](#_Toc434486848)

[5.1 Creation and personalization 22](#_Toc434486849)

[5.1.1 TPM readiness 22](#_Toc434486850)

[5.1.2 Creation 23](#_Toc434486851)

[5.1.3 Personalization 24](#_Toc434486852)

[5.2 Provisioning 25](#_Toc434486853)

[5.3 Maintenance 26](#_Toc434486854)

[5.3.1 Emergency preparedness 27](#_Toc434486855)

[6 Troubleshooting 28](#_Toc434486856)

[6.1 TPM not provisioned 28](#_Toc434486857)

[6.2 TPM in lockout 28](#_Toc434486858)

[7 Summary 29](#_Toc434486859)

[8 Appendix 30](#_Toc434486860)

[8.1 Glossary 30](#_Toc434486861)

[8.2 Traditional smart card basics 30](#_Toc434486862)

[8.3 Virtual smart card non-exportability details 31](#_Toc434486863)

[8.4 Virtual smart card anti-hammering details 32](#_Toc434486864)

[9 Virtual smart cards on consumer devices for corporate access 34](#_Toc434486865)

[9.1 TPM ownerAuth in registry 34](#_Toc434486866)

[9.2 Managed cards 34](#_Toc434486867)

[9.2.1 Card creation 35](#_Toc434486868)

[9.2.2 Card management 35](#_Toc434486869)

[9.2.3 Certificate management 35](#_Toc434486870)

[9.3 Unmanaged cards 37](#_Toc434486871)

[9.3.1 Card creation 37](#_Toc434486872)

# Introduction

## Purpose

### Overview

The goal of this document is to present an overview of Trusted Platform Module (TPM) virtual smart cards (VSCs) as an option for strong authentication. It is intended not only to provide the means for evaluating VSC use in an enterprise deployment, but also to provide the information necessary to deploy and manage.

### Audience

This document is intended for those who may be interested in deploying virtual smart cards within their organization. Additionally, information about the deployment of VSCs is included for those who have decided to proceed with deployment.

## Options for authentication

The following sections present several commonly used options for authentication and their respective strengths and weaknesses.

### Passwords

A password is a secret string of characters, tied to a user’s identification credentials (e.g. a user name), which establishes the user’s identity. The most commonly used form of authentication, passwords, is also the weakest form. In a system where passwords are used as the sole method of user authentication, only individuals who know their passwords are considered valid users. Password authentication places a great deal of responsibility in the hands of the user: chosen passwords must be sufficiently complex so as not to be easily guessed but simple enough to be committed to memory and not stored in any physical location. Even if this balance is successfully achieved, a wide variety of attacks exist whereby an adversary can acquire a user’s password and take over that person’s identity, such as brute force attacks, eavesdropping, and social engineering tactics. Once a password is compromised, a user will often not realize this, and therefore, it is easy for an attacker to maintain access to a system once a valid password has been obtained.

### One-time passwords (OTPs)

A one-time password is similar to a traditional password, but it is more secure in that it can be used only once to authenticate a user. The method for determining each new password varies by implementation; however, assuming secure deployment of each new password, OTPs have several advantages over the classic password model of authentication. Most importantly, if a given OTP token is intercepted in transmission between the user and the system he or she is accessing, the interceptor cannot use it for any future transactions. Similarly, if an adversary obtains a valid user’s OTP, he or she will have much more limited access to the system (only one session) than with a traditional password.

### 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 with them to access the system, in addition to knowing the PIN, which provides access to the smart card. Smart cards have three key 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, another feature of smart cards) actually happen in a crypto processor on the card, so malicious software on the host computer cannot observe 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 unwelcome individual to gain and maintain access to a system. Most importantly, access to a smart card−protected system requires that users both have a valid card *and* know the PIN that provides access to that card, and 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 exists, only one individual can use his or her logon credentials at a time and will quickly notice if the card has been lost or stolen. This reduces the risk window of credential theft hugely 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 misplaced or stolen.

## Virtual smart cards as an option

To address these issues, Microsoft has developed a technology that provides the security of smart cards while reducing material and support costs. Virtual smart cards (VSCs) emulate the functionality of traditional smart cards, but instead of requiring the purchase of additional hardware, they utilize technology that users already own and are more likely to have with them at all times. Theoretically, any device that can provide the three key properties of smart cards (non-exportability, isolated cryptography, and anti-hammering) can be commissioned as a VSC, though the Microsoft virtual smart card platform is currently limited to the use of the Trusted Platform Module (TPM) chip onboard most modern computers. This document will mostly concern TPM virtual smart cards.

Virtual smart cards utilizing a TPM provide the three main security principles of traditional smart cards (non-exportability, isolated cryptography, and anti-hammering, as discussed above), while also being less expensive to implement and more convenient for users. Since many corporate computers will already have a TPM built in, there is no cost associated with purchasing new hardware, and the user’s possession of a computer is equivalent to the possession of a smart card; a user’s identity cannot be assumed from any other computer without administrative provisioning of further credentials. Thus, two-factor auth is achieved: the user must both have a computer set up with the virtual smart card *and* know the PIN necessary to use the VSC.

In the rest of this document, you will find further technical and functional details of virtual smart cards and associated risks, as well as presenting guidelines and scenarios for the use and deployment of TPM VSCs.

# Comparing virtual smart cards with conventional smart cards

Virtual smart cards expose the cryptographic capabilities of devices already in possession of users for use with strong, two-factor authentication. The VSC platform is designed to make VSCs operate with the same functionality and application-level APIs as conventional smart cards. This section provides an overview of the technical and functional similarities and differences between smart cards and their virtual counterpart, as well as address the relative security and cost of the two options.

## Technical

Virtual smart cards function much as conventional smart cards but differ in that they protect private keys by using the TPM of the computer instead of smart card media. The TPM is utilized through a virtualized smart card and reader, and so appears to applications as a conventional smart card. Private keys on the virtual smart card are protected, not by isolation of physical memory, but rather, by the cryptographic capabilities of the TPM: all sensitive information stored on a smart card is encrypted by using the TPM and then stored on the hard drive in its encrypted form. Since all cryptographic operations occur in the secure, isolated environment of the TPM, and the unencrypted private keys are never used outside of this environment, they remain secure from any malware on the host (as with conventional smart cards). Additionally, if the hard drive is compromised in some way, an attacker will not be able to access keys stored on the VSC, as they are securely encrypted by using the TPM and may be further protected by BitLocker® drive encryption.

Virtual smart cards maintain the three key properties of conventional smart cards:

* **Non-exportability:** Since all private information on the VSC is encrypted by using the host machine’s TPM, it cannot be used on a different machine with a different TPM. Additionally, TPMs are designed to be tamper-resistant and non-exportable themselves, so an adversary cannot reverse engineer an identical TPM or install the same one on a different machine.
* **Isolated cryptography:** TPMs provide the same properties of isolated crypto offered by conventional smart cards, and this is utilized by VSCs. When used, unencrypted copies of private keys are loaded only within the TPM and never into memory accessible by the operating system. All cryptographic operations with these private keys occur inside the TPM.
* **Anti-hammering:** If a user enters a PIN incorrectly, the virtual smart card responds by using the anti-hammering logic of the TPM, which rejects further attempts for a period of time instead of blocking the card. This is also known as *lockout*.

## Functional

The Microsoft virtual smart card system has been designed to closely mimic the functionality of actual smart cards. The most striking difference to the end user, however, is that the virtual smart card is essentially a smart card that is *always* inserted into the computer. There is no methodology for exporting the user’s virtual smart card for use on other machines (thus the security of VSCs), but should a user require access to network resources on multiple machines, multiple virtual smart cards can be issued for that user on different machines. Additionally, a machine that is shared among multiple users can host multiple virtual smart cards for different users.

The basic user experience of a virtual smart card is as simple as using a password to access a network—since the smart card is loaded by default, all the user must do to gain access is enter the PIN tied to the card. Users are no longer required to carry with them the cards and readers or take physical action to use the card. Additionally, though the anti-hammering functionality of the VSC is equally secure to that of the smart card, a VSC user will never be required to contact an administrator to unblock the card and will instead just have to wait some period of time (dependent on the specific TPM) before reattempting the PIN entry. Alternatively, the administrator can reset the lockout by providing owner authentication data to the host machine’s TPM.

##  Security

Conventional smart cards and TPM virtual smart cards offer comparable levels of security. They both implement two-factor auth to provide strong authentication for the use of network resources and offer the same benefits and guarantees related to two-factor auth. However, they differ in certain aspects related to their form factors, including the physical security of the device and the practicality of issuing any sort of attack on the device.

Smart cards in their traditional form factor offer little opportunity for acquisition by a potential adversary. Due to their compact and portable design, smart cards are most frequently kept close to their intended user, and any sort of interaction with the card is difficult without committing to some variety of theft. TPM VSCs, however, reside on a user’s computer that may frequently be left unattended, providing an adversary ample opportunity to hammer the device. Though virtual smart cards are just as fully protected from hammering as are conventional smart cards, this accessibility makes the logistics of an attack somewhat simpler. Additionally, as mentioned above, the anti-hammering behavior of a TPM smart card differs in that it only presents a time delay in response to repeated PIN failures, as opposed to a full block.

Mitigating these slight security deficits, however, are several advantages provided by virtual smart cards. Most importantly, a virtual smart card is much less likely to be lost or misplaced compared to a conventional smart card; since VSCs utilize devices that the user already owns for other purposes, they’re no longer a single-purpose accessory and are instead integrated into an otherwise useful device that the user will have more incentive to keep track of. Should the device hosting the VSC be lost or stolen, a user will more immediately notice its loss than would he or she notice the loss of a conventional smart card—employees are much more likely to use their corporate laptop over a long weekend than a smart card, for example. Once the device has been identified as lost, the user can notify the administrator of the system who can revoke the certificate associated with the VSC on that device, and thus preclude any future unauthorized access from that machine (should the PIN for the VSC be compromised).

## Cost

In a traditional smart card situation, a company that wants to deploy the technology will need to purchase both smart cards and smart card readers for all employees. Though relatively cheap 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; these machines are relatively common on the modern 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.

## Smart card vs. virtual smart card summary

|  |  |
| --- | --- |
| Conventional smart cards | TPM virtual smart cards |
| Protect private keys by using the built-in crypto functionality of the card. | Protect private keys by using the crypto functionality of the TPM. |
| Store private keys in isolated non-volatile memory on the card, access them only from the card, and never allowing operating system access. | Store encrypted private keys on the hard drive. The encryption ensures that these keys can only be decrypted and used on the TPM itself, not in operating system‒accessible memory.  |
| Non-exportability guaranteed by the card manufacturer, who can claim the isolation of private information from operating system access. | Non-exportability guaranteed by the TPM manufacturer, who can claim the inability of an adversary to replicate or remove the TPM. |
| Cryptographic operations are performed with and isolated within the built-in capabilities of the card. | Cryptographic operations are performed on and isolated uponthe TPM of the user’s computer. |
| Anti-hammering is provided by the card itself: after a certain number of failed PIN entry attempts, the card will block itself to further access until administrative action. | Anti-hammering is provided by the TPM: successive failed attempts increase the device lockout, or the time the user has to wait before trying again. This can be reset by an administrator. |
| Users must carry their smart card and smart card reader with them for access to network resources. | Users never needs more than their TPM-enabled computer for strong authentication into the network. |
| Credential portability is achieved by inserting the smart card into smart card readers attached to other computers. | Credentials cannot be exported from a given computer, but virtual smart cards can be issued for the same user on multiple computers by using additional certificates. |
| Multiple users can access network resources through the same computer by each inserting their personal smart card. | Multiple users can access network resources through the same computer by each being issued a TPM virtual smart card on that computer. |
| Card is kept on the person of user, making it more difficult for an attacker to access the device and launch a hammering attempt. | Virtual smart card is stored on the user’s computer which may be left unattended, allowing a greater risk window for hammering. |
| Smart card device is generally a single-purpose device, carried explicitly for the purpose of authentication, and easily misplaced or forgotten. | Virtual smart card is installed on a device that has other purposes to the user, and thus the user has greater incentive to be responsible for the device.  |
| If lost or stolen, a user will only notice the absence of the card when he or she needs to log on. | Since the VSC is installed on a device that the user likely needs for other purposes, he or she will notice its loss much more quickly, thus reducing the associated risk window. |
| To deploy a conventional smart card system, a company must invest in smart cards and smart card readers for all employees. | To deploy TPM virtual smart cards, a company must only ensure that all employees have TPM-enabled computers, which are relatively common. |
| Smart card removal policy can be used to affect system behavior when the smart card is removed. For example, the policy can dictate if the user’s logon session is locked or terminated (sign-off) when the user removes the card from the user. | Since a TPM virtual smart card is always inserted and cannot be removed from the reader, the smart card removal policy does not apply to TPM virtual smart card. |

#  Lab setup

## Goal

This section describes how to set up a basic test environment for TPM virtual smart cards. At the end of this lab, the reader will have configured a single TPM smart card to experiment with.

**Important:** This basic test configuration is for test purposes only and not intended for use in a production environment.

## Prerequisites

To participate in this lab, you will need:

* A computer running Windows® 8 with an installed and fully functional TPM.
* A fully ready domain setup with a Windows 8 client connected to the domain.
* Access to any domain server with a fully installed and running certification authority (CA).

## Step one: Create the certificate template

On your domain server, you will need to create a template for the certificate that you will request for the virtual smart card. To do so:

1. On your server, open Microsoft Management Console (MMC). You can type **mmc** from the **Start** menu to access the MMC.
2. Select **File** -> **Add/Remove Snap-in**.
3. In the available snap-ins list, click **Certificate Templates**, and add it.
4. Certificate Templates is now located under Console Root in the MMC window. Double click it to view all available certificate templates.
5. Right-click the **Smartcard Logon** template, and click **Duplicate Template**. 
6. On the **Compatibility** tab, under **Certification Authority**, click **Windows Server 2003**.



1. On the **General** tab:
	1. Specify a name, such as **TPM Virtual Smart Card Logon**.
	2. Set the validity period to the desired value.
2. On the **Request Handling** tab:
	1. Set the **Purpose** to **Signature and smartcard logon**.
	2. Click **Prompt the user during enrollment**.
3. On the **Cryptography** tab:
	1. Set the minimum key size to 2048.
	2. Click **Requests must use one of the following providers**, and then select **Microsoft Base Smart Card Crypto Provider**.
4. On the **Security** tab, add the security group that you want to give enroll access to. If you want to give access to all users, select the **Authenticated users** group and then give them **Enroll** permissions.
5. Click **OK** to finalize your changes and create the new template. Your new template should now appear in the list.
6. Now, add the Certification Authority snap-in to your MMC console (**File** -> **Add/Remove Snap-in**). When asked which computer you want to manage, select the computer on which the CA is located, probably **Local Computer**.
7. In the left panel of the MMC, expand **Certification Authority (Local)**, and then expand your CA within the Certification Authority list.
8. Right-click **Certificate Templates**, and then click **New** -> **Certificate Template to Issue**. 
9. From the list, select the new template that you just created (**TPM Virtual Smart Card Logon**), and then click **OK**. Note that it may take some time before your template replicates to all servers and becomes available in this list.
10. After the template replicates, stop and start the CA. To do so, right-click the CA in the Certification Authority list in the MMC, and then select **All Tasks** -> **Stop Service**. Then, right-click again, and select **All Tasks** -> **Start Service**.


## Step two: Create the TPM virtual smart card

In this step, you will actually create the virtual smart card on the client computer by using the TPM VSC Manager (Tpmvscmgr.exe) in Windows 8.

1. On a domain-joined computer running Windows 8, open a command shell with administrative privileges. To do so, type **cmd** on the **Start** menu, right-click the command prompt program icon, and then click **Run as administrator**. 
2. At the command prompt, type the following, and then press ENTER:

 **tpmvscmgr.exe create /name tpmvsc /pin default /adminkey random /generate**

This will create a virtual smart card with the name **TestVSC**, omitting the unlock key, and generating the file system on the card. (For further use of Tpmvscmgr.exe, see step 4.1.)

1. You will be prompted for a PIN. Enter a PIN that is at least 8 characters in length and confirm.
2. Wait several seconds for the process to finish. Upon completion, Tpmvscmgr.exe will notify you of the device instance ID for the TPM VSC. Store this ID for later reference, as you will need it to manage or remove the VSC.

## Step three: Enroll for the certificate on the TPM VSC

To become fully functional, the virtual smart card must be provisioned with a logon certificate. To do so:

1. Open the Certificates console (type **certmgr.msc** on the **Start** menu).
2. Right-click **Personal**, and then click **All Tasks** -> **Request New Certificate**. 
3. Follow the prompts and when offered a list of templates, select the **TPM Virtual Smart Card Logon** check box (or whatever you named the template in step one). 
4. If prompted for a device, select the Microsoft virtual smart card corresponding to the one you created in the previous section. It would show as **Identity Device (Microsoft Profile)**.
5. Enter the PIN for the TPM smart card that you entered when you created the VSC, and then click **OK**.
6. Wait for the enrollment to finish, and then click **Finish**.

The virtual smart card can now be used as an alternative credential to log on to your domain. To verify that your virtual smart card configuration and certificate enrollment were successful, log out of your current session, then log back on. When you log back on you will either see the new icon for the new TPM virtual smart card on the logon screen or be automatically directed to the TPM smart card logon dialog box. Click the icon, if necessary, enter your PIN, and then click **OK**. You should be logged on to your domain account.

# Virtual smart card use

## Version of TPM supported

Any TPM that adheres to Trusted Computing Group (TCG) specification version 1.2 and later is supported for use as a virtual smart card. For more information, see the [TPM Main Specification](http://www.trustedcomputinggroup.org/resources/tpm_main_specification).

## Using Tpmvscmgr.exe

To allow end user creation and deletion of TPM virtual smart cards, included in-box, with Windows 8 is the Tpmvscmgr.exe utility. Following is a brief usage guide for this tool.

**Tpmvscmgr.exe** – allows creation and deletion of TPM virtual smart cards. Must be run with administrative privileges. For alphanumeric inputs, the full 127 character ASCII set is allowed.

**create** – sets up a new virtual smart card on the user’s system. Returns the instance ID of the newly created card, for later reference in deletion. The instance ID is of the format **ROOT\SMARTCARDREADER\000*n*** where ***n*** starts from 0 and is increased by 1 each time you create a new virtual smart card.

**/name** – parameter indicates the name of the new virtual smart card. The /name parameter is a required field for the create command.

**/AdminKey** – parameter indicating desired administrator key that can be used to reset the PIN of the card if the user forgets the PIN.

 **DEFAULT** specifies the default value of 010203040506070801020304050607080102030405060708.

 **PROMPT** will result in the user getting prompted to enter a value for the administrator key.

 **RANDOM** will result in random admin key getting set for the card that is not returned back to the user. This will create a card that may not be manageable by using smart card management tools.

 The admin key must be entered as 48 hexadecimal characters.

**/PIN** – parameter indicating desired user PIN value.

 **DEFAULT** specifies the default PIN of 12345678.

 **PROMPT** results in the user getting prompted to enter a PIN on the command line. The PIN must be a minimum 8 characters in length and can accept digits, characters, and special characters.

 **/PUK** – parameter indicating the desired PUK (PIN Unblocking Key) value. If the parameter is omitted, the card is created without a PUK.

 **DEFAULT** specifies the default PUK of 12345678.

 **PROMPT** results in the user getting prompted to enter a PUK on the command line. The PIN must be a minimum 8 characters in length and can accept digits, characters, and special characters.

**/generate** – when specified, generates the files in storage necessary for the function of the virtual card. If the /generate parameter is omitted, it is equivalent to creating a card without this file system. A card without a file system can only be managed by a smart card management system such as Microsoft FIM CM.

**/machine** – specify the name of the remote computer on which the virtual smart card must be created. This can be used in domain environment only and relies on DCOM. For the command to succeed in creating a virtual smart card on a different computer, the caller must be present in the local administrators group on the remote computer.

**destroy** – securely deletes a virtual smart card from the user’s system. Care must be taken while deleting a virtual card. Once deleted, the virtual smart card cannot be recovered.

**/instance** – parameter specifies the instance ID of the virtual smart card to be removed, as output by Tpmvscmgr.exe upon creation of the card. The /instance parameter is a required field for the destroy command.

## Programmatic management of virtual smart cards

Virtual smart cards can also be created and deleted by using APIs. For more information, see the [TpmVirtualSmartCardManager](http://msdn.microsoft.com/en-us/library/windows/desktop/hh707171%28v%3Dvs.85%29.aspx) and [RemoteTpmVirtualSmartCardManager](http://msdn.microsoft.com/en-us/library/windows/desktop/hh707166%28v%3Dvs.85%29.aspx) classes and [ITpmVirtualSmartCardManager](http://msdn.microsoft.com/en-us/library/windows/desktop/hh707160%28v%3Dvs.85%29.aspx) and [ITPMVirtualSmartCardManagerStatusCallBack](http://msdn.microsoft.com/en-us/library/windows/desktop/hh707161%28v%3Dvs.85%29.aspx) interfaces.

You can use APIs introduced in Windows 8.1 and Windows Server 2012 R2 in the Windows.Device.SmartCards namespace to build Windows Store apps to manage the full lifecycle of virtual smart cards. For information how to build an app to do this, see Strong Authentication: Building Apps That Leverage Virtual Smart Cards in Enterprise, BYOD, and Consumer Environments | Build 2013 | Channel 9 (http://channel9.msdn.com/Events/Build/2013/2-041).

The following table describes these features which can be developed in a Windows Store app:

|  |  |  |
| --- | --- | --- |
| Feature | Physical smart card | Virtual smart card |
| Query and monitor smart card readers | Yes | Yes |
| List availablesmart cards in a reader, retrieve the card name, and retrieve card ID | Yes | Yes |
| Verify if the admin key of a card is correct | Yes | Yes |
| Provision (or reformat) a card with a given card ID | Yes | Yes |
| Change the PIN by entering the old PIN and then specifying the new PIN | Yes | Yes |
| Change the admin key, reset the PIN, unblock the smart card using a challenge/response | Yes | Yes |
| Create a virtual smart card | Not applicable | Yes |
| Delete a virtual smart card | Not applicable | Yes |
| Set PIN policies | No | Yes |

For information about these Windows APIs, see:

* Windows.Devices.SmartCards namespace (Windows) (<http://msdn.microsoft.com/library/windows/apps/windows.devices.smartcards.aspx>)
* Windows.Security.Cryptography.Certificates namespace (Windows) <http://msdn.microsoft.com/library/windows/apps/windows.security.cryptography.certificates.aspx>

## Distinguishing TPM virtual smart card from physical smart cards

The TPM virtual smart card has an icon that is different from a regular smart card. This helps the user visually distinguish the TPM virtual smart card from physical smart cards. The following icon is displayed during logon and various other screens that require the user to enter the PIN for TPM virtual smart card.



The TPM virtual smart card is labeled **Security Device** in the user interface.

## Number of virtual smart cards on a computer

Windows supports a maximum of 10 smart cards connected to a computer at a time. This includes physical and virtual smart cards combined. You can create more than 1 virtual smart card; however, after creating more than 4 virtual smart cards, you may start to notice performance degradation. Since all smart cards appear as always inserted, if more than 1 person share a computer, each person will be able to see all virtual smart cards created on that computer. If the user knows the PIN values for all smart cards, the user will also be able to use them.

## Number of certificates on a virtual smart card

A single TPM virtual smart card can contain 30 distinct certificates along with the corresponding private keys. Users can continue to renew certificates on the card until the total number of certificates on a card exceed 90. The reason why the total number of certificates is different from the total number of private keys is that sometimes the renewal can be done with the same private key in which case a new private key is not generated.

## PIN, PUK, and admin key requirements

The PIN and the PUK must be a minimum of 8 characters. It need not contain only digits though the name suggests that it is a Personal Identification Number. You can enter digits, letters, and special characters.

The admin key must be entered as 48 hexadecimal characters. It is a 3-key triple DES with ISO/IEC 9797 padding method 2 in CBC chaining mode.

## Changing the PIN

The PIN for TPM virtual smart card can be changed by pressing Ctrl+Alt+Del, and then selecting the TPM virtual smart card under **Signin options**, if it is not already selected.

## Authentication

### Use case: Two-factor auth‒based remote access

After a user has a fully functional TPM virtual smart card, provisioned with a logon certificate, the logon certificate is used to gain strongly authenticated access to corporate resources. With the proper certificates provisioned on the virtual card, the user need only provide the PIN to the VSC, as if it were a conventional smart card, to be logged on to the domain.

In practice, this is as easy as entering a password to access the system. Technically, it is far more secure. Using the virtual smart card to access the system proves to the domain that the user requesting authentication both knows the VSC PIN and has possession of the personal computer upon which the card has been provisioned. Since this request could not have possibly originated from a system other than the system certified by the domain for this user’s access, and the user could not have initiated the request without knowing the PIN, strong, two-factor authentication is established.

### Use case: Client authentication

Virtual smart cards can also be used in client authentication, over SSL or some similar technology. Similar to domain access with a VSC, an authentication certificate can be provisioned to the virtual smart card and provided to a remote service as requested in client authentication. This again adheres to the principles of two-factor authentication, because the certificate is only accessible from the computer hosting the VSC, and the user is required to enter the PIN for initial access to the card.

### Use case: Virtual smart card redirection for remote desktop connections

The concept of two-factor authentication associated with virtual smart cards relies on the proximity of the user to the computer he or she is accessing domain resources through. Therefore, when a user remotely connects to a computer that is hosting virtual smart cards, the VSCs located on the remote computer *cannot* be used during the remote session. However, the VSCs stored on the connecting computer (which is under *physical* control of the user) are loaded onto the remote computer and can be used as if they were installed using the remote computer’s TPM. This extends a user’s privileges to the remote computer, while maintaining the principles of two-factor authentication. To support this functionality the minimum version of Windows on the remote server must be Windows 7 SP1, Server 2008 R2 SP1, or later versions.

### Windows To Go and virtual smart cards

Virtual smart cards work well with Windows To Go where a user may boot into Windows 8 from a compatible USB drive. A virtual smart card can be created for the user in this case and will be tied to the TPM on the physical host computer to which the USB drive is connected. When the user boots the operating system from a different physical computer, the virtual smart card will not be available. This can be used for scenarios where a single physical computer is shared by many users. Each user can be given a Windows To Go USB drive that has the virtual smart card provisioned for the user. This way, the user will only be able to access his or her virtual smart card.

## Confidentiality

### Use case: S/MIME email encryption

Conventional smart cards are designed to hold private keys that can be used for email encryption and decryption, and this functionality carries over to virtual smart cards as well. By encrypting emails using S/MIME with a user’s public key, the sender of an email can be assured that only the person with the corresponding private key will be able to decrypt the email. This assurance is a result of the non-exportability of the private key—it never exists within reach of malware or any adversary and remains protected by the TPM even during decryption.

### Use case: BitLocker for data volumes

Microsoft BitLocker technology makes use of symmetric-key encryption for protecting the content of a user’s hard drive, ensuring that if the physical ownership of a hard drive is compromised, an adversary will not be able to read data off the drive. The key used to encrypt the drive can be stored on a virtual smart card, which necessitates not only knowledge of the VSC PIN to access the drive, but also possession of the computer hosting the TPM virtual smart card. If the drive is obtained without access to the TPM that hosts the virtual smart card, any brute force attack will be very difficult.

BitLocker can also be used to encrypt portable drives, a process in which keys stored on virtual smart cards can also be employed. In this scenario, unlike using BitLocker with a traditional smart card, the encrypted drive can only be used when connected to the host of the VSC used to encrypt the drive, because the BitLocker key is only accessible from this computer. However, this can be useful for ensuring the security of backup drives and personal storage purposes outside the main hard drive.

## Integrity

### Use case: Signing data

To verify one’s authorship of certain data, the user can sign it by using a private key stored on the virtual smart card. Digital signatures assert non-repudiation, or confirmation of integrity and origin of the data. This non-repudiation is as easily compromised as is an individual’s private key; however, if the key is stored in operating system‒accessible memory, it can be acquired by malware and used by adversaries to modify already signed data, or even spoof the identity of the key’s owner. However, if this key is stored on a virtual smart card, it can only be used to sign data on the host computer and not exported (either intentionally or unintentionally, as with malware theft) to other systems, making digital signatures far more secure than with other methods for private key storage.

# Deployment of virtual smart cards

Traditional identity devices, such as conventional smart cards, follow a predictable lifecycle in any deployment, as shown in the following diagram.



With physical devices, the device itself is created by a dedicated manufacturer, and then purchased by the corporation that will ultimately deploy it. The device then passes through the personalization stage, where its unique properties are set—in the case of smart cards, these properties are the admin key, PIN, and PUK of the card, as well as its physical appearance. In device provisioning, the identity device is loaded with whatever certificates are required for use (such as a logon certificate). After provisioning the device, it is ready for use, and the deployment must simply be maintained—cards must be replaced when lost or stolen; PINs must be reset when forgotten by the user; and so on. Finally, devices must be retired upon exceeding intended lifetime or when an employee leaves the company.

In the following sections, the lifecycle of identity devices is discussed in the context of TPM virtual smart cards, including the process and requirements for each stage. Many phases are best executed by using a card management solution, and these sections will discuss this process and what is accomplished with either an in-house or provided solution.

## Creation and personalization

### TPM readiness

Because the security provided by a TPM virtual smart card relies on the proper functioning of the computer’s TPM, this must be fully provisioned on the intended host of the VSC. The TPM Provisioning Wizard—launched from the TPM Management Console (tpm.msc)—will take the user through all steps to ready the TPM for use. For the final state of the TPM, as it applies to virtual smart cards, several things are important:

* **Enabled/Activated:** TPMs come built in with many industry-ready computers currently on the market, but they are often not enabled and activated by default. In some cases, the TPM must be enabled and activated through the BIOS.
* **Ownership Taken:** As a part of provisioning the TPM, an owner password is set to manage the TPM in the future as well as the Storage Root Key (SRK) is established. To be able to reset the anti-hammering for VSC use, either the user or a corporate (domain) administrator must have access to the TPM owner password. For corporate use of TPM virtual smart card, we recommend that the corporate domain administrator restrict access to the TPM owner password by disallowing storage of it in the local registry. Instead, it should be stored in Active Directory®. For more information, see [Trusted Platform Module Technology Overview](http://technet.microsoft.com/library/jj131725.aspx). For cases where the TPM ownership is taken in Windows Vista®, the TPM will need to be cleared and reinitialized.
* **Managed:** By using this owner password, it is possible to change the owner password (manage ownership) and reset the lockout of the chip (manage anti-hammering logic for VSCs).

Sometimes a TPM may present itself in reduced functionality mode. This could occur, for example, when the operating system is not able to determine if the owner password is available to the user or not. In those cases, the TPM may be used for creating a virtual smart card, but it is strongly recommended to bring the TPM to a fully ready state so that any unexpected circumstances will not leave the user blocked from using the computer.

For smart card deployment management tools that want to check the status of a TPM before attempting to create a TPM virtual smart card, they can do so using the TPM WMI interface.

Depending on the setup of the computer designated for TPM VSC installation, it may be necessary to provision the TPM before continuing with the virtual smart card deployment. For more information about provisioning, see the “Troubleshooting” section of this document.

For more information about managing TPMs by using built-in tools in Windows 8, see [Windows 8 TPM Group Policy Settings](http://technet.microsoft.com/library/jj679889.aspx).

### Creation

A TPM virtual smart card is created as a simulation of a physical smart card, which uses the TPM to provide the same functionality as conventional smart card hardware. It appears within the operating system as a conventional smart card that is always inserted. Windows 8 presents a virtual card reader and virtual card to applications with the same interface as conventional smart cards, but messages to and from the VSC are translated to TPM commands, which ensures the integrity of the virtual smart card through the three properties of smart card security:

* **Non-exportability:** All information stored on the VSC is encrypted with the TPM.
* **Isolated cryptography:** Cryptographic operations can be executed on the TPM itself, so private information used for encryption/decryption is never revealed to any applications.
* **Anti-hammering:** The anti-hammering logic of the TPM protects virtual smart cards from brute-force attacks.

There are several options for creating virtual smart cards, depending on the size and budget of the deployment. The lowest cost option is using Tpmvscmgr.exe to create cards individually on users’ computers, as described in the “Virtual smart card use” section. Alternatively, a virtual smart card management solution can be purchased to more easily accomplish VSC creation on a larger scale and aid in further phases of deployment. VSCs can either be created on computers that have yet to be handed off to the employee, or on those already in employees’ possession. In either approach, there should be some central control over personalization and provisioning. If a computer is intended for use by multiple employees, multiple virtual smart cards can be created on a computer.

### Personalization

During virtual smart card personalization, the values for the admin key, PIN, and PUK are assigned. As with a conventional card, recording the admin key is important for being able to reset the PIN or wipe the card in the future. If a PUK is set, however, the admin key can no longer be used to reset the PIN.

Because the admin key is critical to the security of the card, it is important to consider the deployment environment and decide upon the proper admin key setting strategy. Options for these strategies include:

* **Uniform:** Admin keys for all virtual smart cards deployed are the same. While this makes the maintenance infrastructure easy (only one key needs to be stored), it is highly insecure. This strategy may be sufficient for very small organizations, but if the admin key is compromised, all cards using this key must be re-issued.
* **Random, not stored:** Admin keys are assigned randomly for all virtual smart cards and not recorded. This is a valid option if the deployment administrators do not require the ability to reset PINs, and instead prefer to delete and re-issue cards to achieve this. This could also be a viable strategy if the admin prefers to set the cards’ PUK values and use this to reset PINs, if necessary.
* **Random, stored:** Admin keys are assigned randomly and stored in some central location. This is secure on a large scale—unless the admin key database is compromised, each card’s security is independent of the others’.
* **Deterministic:** Admin keys are the result of some function on known information. For example, the user ID, the card ID values could be used as seeds for randomly generating some data that can be further processed through a symmetric encryption algorithm by using a secret to generate an admin key. This admin key can be similarly re-generated when needed and not need storage. The security of this method relies on the security of the secret used.

Though the admin key and PUK can both provide unlocking/resetting functionality, they do so in different ways. The PUK is a PIN that must simply be entered on the computer to enable user PIN reset, while the admin key methodology takes a challenge response approach. In the latter situation, the card provides a set of random data that the user reads (after verification of identity) to the deployment admin. The admin then encrypts the data with the admin key (obtained as above) and gives the encrypted data back to the user. If the encrypted data matches that produced by the card during verification, the card will allow PIN reset. Since the admin key is never in the hands of anyone other than the deployment administrator, it cannot be intercepted or recorded by any other party (including the employee), and thus has significant security benefits beyond using a PUK—an important consideration during the personalization process.

TPM virtual smart cards can be personalized on an individual basis during creation with the Tpmvscmgr.exe tool, or a purchased management solution could incorporate personalization into an automated routine. A further advantage of such a solution is the automated creation of admin keys—Tpmvscmgr.exe allows users to create their own admin keys, which can be detrimental to the security of the VSC (as discussed above).

## Provisioning

Provisioning is the process of loading specific credentials onto a TPM virtual smart card. These credentials consist of certificates created to give users access to a specific service, such as domain logon. A maximum of 30 certificates is allowed on each virtual smart card. As with conventional smart cards, several decisions must be made regarding the provisioning strategy based on the environment of the deployment and the desired level of security.

A high assurance level of secure provisioning requires absolute certainty of the individual’s identity who is receiving the certificate. Therefore, one method of high assurance provisioning is utilizing previously provisioned strong credentials, such as a physical smart card, for validation of identity during provisioning. In-person proofing at enrollment stations is another option—as an individual can easily and securely prove his or her identity with a passport or driver’s license—though this can become infeasible on a larger scale. To achieve a similar level of assurance, a large deployment can implement an enroll-on-behalf-of (EOBO) strategy, in which each employee is enrolled with his or her credentials by a superior who can personally verify the person’s identity. This creates a chain of trust that ensures that each individual is checked against his or her proposed identity in person but without the administrative strain of provisioning all VSCs from a single central enrollment station.

For deployments in which a high assurance level is not a primary concern, self-service solutions can be utilized. These can include going to an online portal to obtain credentials, or simply enrolling for certificates by using Certmgr.msc (as in the lab), depending on the deployment. It must be kept in mind, however, that VSC authentication will only be as strong as the method of provisioning—if weak domain credentials (such as a password alone) are used to request the authentication certificate, VSC authentication will be equivalent to using the password itself, and thus the benefits of two-factor authentication are lost.

Both high assurance and self-service solutions approach VSC provisioning assuming that the user’s computer has been issued prior to the VSC deployment, but this is not always the case. If virtual smart cards are being deployed with new computers, they can be created, personalized, and provisioned on the computer, all before the user comes into contact with that computer. In this situation, provisioning becomes relatively simple, but checks must be put in place to ensure that the recipient and user of the computer is the individual expected during provisioning. This can be accomplished by requiring the employee to set the initial PIN under supervision of the deployment admin or manager.

A further consideration beyond methods of provisioning is the longevity of credentials supplied to virtual smart cards. This choice must be based on the risk appetite of the organization. While longer lived credentials are more convenient, they are also more likely to become compromised during their greater lifetime. To decide upon the appropriate lifetime of credentials, the deployment must take into account the vulnerability of their cryptography (how long it can take to crack the credentials), as well as the likelihood of attack.

Should a given virtual smart card be compromised, as with a lost or stolen laptop, the organization should also be able to revoke the associated credentials. This requires some record of which credentials match which user and computer, functionality that does not exist natively in Windows. Deployment admins may want to consider add-on solutions to maintain such a record.

## Maintenance

Maintenance is by far the largest portion of the virtual smart card lifecycle and one of the most important considerations from a management perspective. Once created, personalized, and provisioned, VSCs can be used for convenient two-factor auth, but deployment administrators must be aware of several common administrative scenarios. Each of these can be approached with a purchased virtual smart card solution or accomplished on a case-by-case basis with in-house methods.

Renewal of virtual smart card credentials is a regular task necessary to preserve the security of a VSC deployment. Renewal is the result of a signed request from the user, in which he or she specifies the key pair desired for the new credentials. Depending on user choice or deployment specification, the user can request credentials with the same key pair as before, or choose a newly generated key pair. When renewing with a previously used key, no extra steps are required, because a certificate with this key was issued strongly during the initial provisioning. However, when renewing with a new key, the same steps taken during provisioning to assure the strength of the credential (in person proofing, EOBO, etc.) must be taken. Renewal with new keys should occur periodically to counter sophisticated long-term cracking attempts, but when this is done, steps must be taken to ensure that the new keys are being used by the expected individual on the same virtual smart card as before.

Resetting virtual smart card PINs is also a frequent necessity, should an employee forget his or her PIN. There are two ways to accomplish this, depending on choices made earlier in deployment: using a PUK, if the PUK is set, or using challenge/response with the admin key (each discussed in the earlier “Personalization” subsection). Before resetting the PIN, however, the user’s identity must be verified by using some means other than the card, likely most easily the verification method used during initial provisioning (e.g. in person proofing). This is necessary in user-error scenarios when the PIN has been forgotten, but it should never be employed if the PIN is compromised. As above, the level of vulnerability after exposure of the PIN is difficult to identify, so the entire card should be reissued.

A frequent precursor to PIN reset is the necessity of TPM lockout reset, as the TPM anti-hammering logic will be engaged with multiple PIN entry failures for a virtual smart card. This is currently device-specific.

The final aspect of virtual smart card management is retiring cards when they are no longer needed. When an employee leaves the company, it is desirable to revoke domain access, and revoking logon credentials from the certification authority (CA) accomplishes this goal. However, the card should also be reissued if the same computer is to be used for other employees without operating system reinstall. Reusing the former card may allow the ex-employee to change the PIN post-employment and/or hijack the certificates belonging to the new user for unauthorized domain access. Should the employee take the VSC-enabled computer, however, it is only necessary to revoke the certificates stored on his or her card.

### Emergency preparedness

#### Card re-issuance

The most common scenario is the reissuance of virtual smart cards, which can be necessary if the operating system is reinstalled, or the card is compromised in some manner. Reissuance is essentially the recreation of the card from the ground up—establishing a new PIN and admin key and provisioning a new set of associated certificates. This is an immediate necessity when a card is compromised, for example, if the VSC-protected computer is exposed to an adversary who may have access to the correct PIN, as reissuance is the most secure response to an unknown exposure of the card’s privacy. Additionally, reissuance is necessary after an operating system reinstallation, because the virtual smart card device profile is removed with all other user data upon reinstall.

#### Blocked virtual smart card

The anti-hammering behavior of a TPM virtual smart card is different from a physical smart card. As previously mentioned, a physical smart card blocks itself after the user enters the wrong PIN a few times. A TPM virtual smart card, however, behaves differently. It goes into a timed delay after the user enters the wrong PIN a few times. Once the TPM is in the timed delay mode, when the user attempts to use the TPM virtual smart card, the user is notified that the card is blocked. Furthermore, if integrated unblock is enabled, the user may be shown the user interface to unblock the virtual smart card. Unblocking the virtual smart card DOES NOT reset the TPM lockout. The user will need to perform an extra step to reset the TPM lockout or wait for the timed delay to expire.

Introduced in Windows 8.1 and Windows Server 2012 R2 , the virtual smart card works with the behavior of the TPM to allow for multiple wrong PIN attempts without triggering the anti-hammering protection of the TPM. If the user enters the wrong PIN 5 consecutive times for a virtual smart card, the card gets blocked. Each wrong PIN is still checked against the TPM. Once the card is blocked, it has to be unblocked using the admin key or the PUK. Typically the unblock process is managed by a virtual smart card management system.

For more information about the TPM’s anti-hammering protection capabilities, see “8.4 Virtual smart card anti-hammering details” in this document.

# Troubleshooting

A TPM virtual smart card can fail during its creation or use for a few reasons described in the following sections.

## TPM not provisioned

For a TPM virtual smart card to function properly, a provisioned TPM must be available on the system. If the TPM is disabled in the BIOS, or is not provisioned with full ownership taken and the Storage Root Key (SRK) established, the TPM virtual smart card creation will fail.

Furthermore, if the TPM is reinitialized after creating a virtual smart card, the card will no longer function and will need to be re-created.

If the TPM ownership was established from a Windows Vista installation, the TPM will not be ready for use as a virtual smart card. The system administrator will need to clear and reinitialize the TPM in order for it to be suitable for creating a TPM virtual smart card.

If the operating system is re-installed, any prior TPM virtual smart cards will no longer be available and will need to be re-created. If the operating system is upgraded, any prior TPM virtual smart cards will be available to use in the upgraded operating system.

##  TPM in lockout

Sometimes, due to frequent incorrect PIN attempts from a user, the TPM may enter the lockout state. To resume using the TPM virtual smart card, it will be necessary to either reset the lockout on the TPM by using the owner password or to wait for the lockout to expire. Unblocking the user PIN alone does not reset the lockout on the TPM. While the TPM is in lockout, the TPM virtual smart card will appear as if it is blocked. Typically, when the TPM enters the lockout state because the user entered an incorrect PIN too many times, it may be necessary to also reset the user PIN by using the card management tools.

Sometimes, it may be necessary to contact Microsoft Technical Support when there are issues preventing you from using the virtual smart card. The Microsoft Technical Support representative may request that you enable tracing or that you look at event logs on the system to diagnose and repair the issues.

# Summary

Virtual smart cards are a new technology from Microsoft that offers comparable security benefits in two-factor authentication with conventional smart cards but more convenience to users and cost during deployment. By utilizing TPM devices that provide the same cryptographic capabilities as traditional smart cards, VSCs accomplish the three key properties of smart cards: non-exportability, isolated cryptography, and anti-hammering.

Virtual smart cards are functionally similar to conventional smart cards, and even appear within Windows 8 as always-inserted smart cards, which can be used for authentication to external resources, protection of data by secure encryption, and integrity through reliable signing. They are easily deployed by using in-house methods or a purchased solution and can become a full replacement for other methods of strong authentication in a corporate setting of any scale.

This document has reviewed the main technical and functional differences between smart cards and VSCs, hoping to aid in the decision to adopt this technology. A lab setup was provided for the evaluation of virtual smart cards and pointers and scenarios for VSC use. Finally, scenarios for issuing and maintaining a deployment of virtual smart cards have been considered. Upon finishing this document, you will have a better idea about whether virtual smart cards are the best choice for your business and will be able to proceed with deployment knowing how to best approach a successful implementation of virtual smart card technology.

# Appendix

## Glossary

**Two-factor auth –** Two-factor authentication, or “what you have and what you know.” Allows authentication based on both physical possession of some object (for example, a smart card) and the knowledge of secret information necessary to use that object (for example, a PIN).

**Hammering –** The attempt to guess the PIN of a smart card with repeated trial and error. To maintain their security, all smart cards (virtual and otherwise) must implement anti-hammering, or some form of protection against this.

**PIN –** Personal Identification Number. In the context of smart cards, the PIN is not necessarily a “number,” but rather any ASCII character series used to gain access to the card.

**PUK –** PIN Unlock Key. Used (if enabled) to change a user’s PIN or to unblock the smart card.

**TPM –** Trusted Platform Module. The isolated, secure cryptographic processor built into many modern computers and the basis of virtual smart card security.

**VSC –** Virtual smart card. Microsoft’s new smart card technology, which uses some preexisting cryptographically secure device to simulate a conventional smart card.

## Traditional smart card basics

In its original form, a smart card is a computing device, most often affixed to an ID card or similarly sized object (this size is regulated by international standards)*.* The smart card itself contains a processor and a small amount of storage, which is tamperproof and isolated from external use or access. This isolated memory makes it possible for the card to generate and/or store some secrets, such as private keys associated with certificates held on the card, separate from storage, which is public to any application accessing the card.

Beyond its function as a storage device, a smart card also has an internal operating system, and it can perform cryptographic operations onboard the device, as well as host custom applications for further functionality.

Smart cards have several capabilities:

* **Authentication:** Before distribution, smart cards are provisioned with a certificate verified by a certification authority (CA), which establishes their validity on a domain. This certificate can then be used for logon to the domain. Smart cards can be similarly used for client authentication over SSL.
* **Protection:** By using the onboard cryptographic capabilities, a smart card can decrypt data, for example, it can allow secure email communication with S/MIME. Because the user’s key pair is stored on the card and all crypto operations are performed by using the card’s CPU, these transactions are completely secure, even from malware on a the user’s computer.
* **Integrity:** Applications can utilize private keys, stored on the smart card device, to sign information, such as emails and/or documents.

In Smart Cards for Windows, this functionality is accessible from any application to any smart card, through either the CryptoAPI (CAPI) or the more recent Crypto Next Generation (CNG) API, collectively referred to as CryptoAPI 2.0 (CAPI2). The customization of the system to respond to differences in hardware occurs at a lower level, the preferred method being a “mini-driver” written by the card manufacturer, which ultimately sends its communication through a device-specific reader driver, to the card itself.

## Virtual smart card non-exportability details

A crucial aspect of TPM VSCs is their ability to securely store and use secret data. Here, “secure” means that the data is non-exportable: it can be accessed and used within the virtual smart card system, but it is meaningless outside of its intended environment. In TPM VSCs, this is ensured with a secure key hierarchy—several chains of encryption originating from the TPM Storage Root Key (SRK), which is generated and stored within the TPM and never exposed outside the chip. This key hierarchy is designed to allow encryption of user data with this key, but it authorizes decryption with the user PIN in such a way that changing the PIN doesn’t require re-encryption of the data.



This diagram illustrates the key hierarchy and the process of accessing the user key. Stored on the hard disk are the user keys and the “smart card key” (encrypted by the SRK) and the authorization key for user key decryption (the “auth key”), encrypted by the public portion of the smart card key. When the user enters a PIN, the use of the decrypted SC key is authorized with this PIN and, if this authorization succeeds, the decrypted SC key is, in turn, used to decrypt the auth key. The auth key is then provided to the TPM to authorize the decryption and use of the user key(s) stored on the virtual smart card. This auth key is the only sensitive data that is used as plaintext outside the TPM, but its presence in memory is protected by the Microsoft Data Protection API (DPAPI), such that before being stored in any way, it is encrypted. All data other than the auth key is processed only as plaintext within the TPM, which is completely isolated from external access.

## Virtual smart card anti-hammering details

The anti-hammering functionality of virtual smart cards relies on the anti-hammering functionality of the TPM enabling the VSC. However, the TPM v1.2 specification (as designed by the Trusted Computing Group) provides very flexible guidelines for responding to hammering, requiring only that the TPM implement some sort of protection against trial-and-error attacks on the user PIN, PUK, and challenge/response mechanism. The Trusted Computing Group (TCG) also specifies that, if the response to attacks involves suspension of proper function of the TPM for some period of time or until administrative action, the TPM must prevent the execution of authorized TPM commands and may prevent the execution of *any* TPM commands, until the termination of the attack response. Beyond time delay and requirement of administrative action, a TPM could also force reboot when an attack is detected, but the TCG allows manufacturers a certain level of creativity in their choice of implementation. Whatever methodology chosen by TPM manufacturers will determine the anti-hammering response of TPM virtual smart cards. Some typical aspects of protection from dictionary attacks include:

1. Allowing only a limited number of wrong PIN attempts before enabling a lockout that enforces a time delay before any further commands are accepted by the TPM. Note: Introduced in Windows 8.1 and Windows Server 2012 R2 , if the user enters the wrong PIN 5 consecutive times for a virtual smart card, which works in conjunction with the TPM, the card gets blocked. Once the card is blocked, it has to be unblocked using the admin key or the PUK.
2. Exponentially increase the time delay as the user enters the wrong PIN so that an excessive number of wrong PIN attempts will quickly trigger long delays in accepting commands.
3. Have a failure leakage mechanism to allow the TPM to reset the timed delays over a period of time. This is useful in cases where a valid user has entered the wrong PIN occasionally (for example, due to complexity of the PIN).

As an example, it will take 14 years to guess an 8-character PIN for a TPM that has the following behavior:

1. Number of wrong PINs allowed before entering into lockout (threshold): 9
2. Time the TPM is in lockout once the threshold has reached: 10 seconds
3. For each wrong PIN after the threshold has been reached, the timed delay doubles.

# Virtual smart cards on consumer devices for corporate access

This section describes a few techniques that can be used to allow an employee to provision a virtual smart card and enroll for certificates that can be used to authenticate the user when the user attempts to access a corporate resource from a device that is not joined to the corporate domain. Furthermore, this section focuses on those devices that do not allow the user to download and run applications from sources other than the Windows Store (such as Windows RT).

For the purpose of this document, two types of virtual smart cards exists on consumer devices—managed and unmanaged. These cards have the following important differences.

|  |  |  |
| --- | --- | --- |
| Operation | Managed card | Unmanaged card |
| PIN reset when the user forgets the PIN | Yes | No, the card has to be deleted and created again. |
| Allow user to change the PIN | Yes | No, the card has to be deleted and created again. |
|  |  |  |

You can use APIs introduced in Windows 8.1 and Windows Server 2012 R2 to build Windows Store apps to manage the full lifecycle of virtual smart cards. For more information, see section “4.3 Programmatic management of creation and deletion of virtual smart cards” in this document.

## TPM ownerAuth in registry

In non-domain joined cases, the TPM ownerAuth is stored in the registry (HKLM). This exposes some threats. Most of the threat vectors are protected by BitLocker. The threat vector that is not protected is the scenario is:

* A thief gets hold of a device with an active local logon session before the device locks itself. The thief could try to brute-force the VSC PIN and get hold of the corporate secrets.
* A thief gets hold of a device with an active VPN session. All bets are off in this case.

The proposed mitigation for the above scenarios is to reduce the auto-lockout time from 5 minutes to 30 seconds in case of inactivity by using EAS policies. The right expectation can be set around auto-lockout while provisioning virtual smart cards. The EAS policy configuration change can take care of both the above scenarios. If an enterprise wants to go a step further, they can also configure a setting to remove the ownerAuth from the local machine.

For configuration information about the TPM ownerAuth registry key, see the "Configure the level of TPM owner authorization available to the operating system" section in [Windows 8 TPM Group Policy Settings](http://technet.microsoft.com/library/jj679889.aspx).

## Managed cards

A managed card is a card that can be serviced by the IT administrator (or other designated role). It allows the IT administrator to have influence or complete control over specific aspects of the card from its creation to deletion. To manage these cards, a smart card deployment management tool is often required.

### Card creation

A blank virtual smart card can be created by the user by using Tpmvscmgr.exe, a built-in tool, executed from a command prompt running with administrative privileges (elevated command prompt). This card will need to be created with well-known parameters (i.e. the default values) and should be left unformatted (i.e. the /generate option should not be specified).

The following command will create the card that can be later managed by a smart card management tool launched from another computer (as explained in the next section):

tpmvscmgr.exe create /name “VirtualSmartCardForCorpAccess” /AdminKey DEFAULT /PIN PROMPT

Alternatively, instead of using a default admin key, one can enter an admin key on the command line:

tpmvscmgr.exe create /name “VirtualSmartCardForCorpAccess” /AdminKey PROMPT /PIN PROMPT

In either case, the card management system needs to be aware of the initial admin key used so that it can take ownership of the card and change the admin key to a value that is only accessible through the card management tool operated by the IT administrator. For example, when the default value is used, the admin key is set to: 010203040506070801020304050607080102030405060708

### Card management

After the card is created, the user will need to open a remote desktop session to an enrollment station (for example, a computer that is joined to the domain). Because smart cards connected to a client computer are available for use in the remote desktop session, the user can launch a card management tool inside the remote session that can take ownership of the card and provision it for use by the user. This will require that a user is allowed to establish a remote desktop connection from a non-domain-joined computer to a domain-joined computer. This may require specific network configuration (IPsec policies) that is beyond the scope of this document.

When the user is in need to reset the PIN or change the PIN, the user will need to use the remote desktop session to complete these operations by using either the built-in tools for PIN unblock and PIN change or through the smart card management tool.

### Certificate management

##### Certificate issuance

Users can enroll for certificates from within a remote desktop session that is established to provision the card. This process can also be managed by the smart card management tool that the user runs when connected to the remote desktop session. This model works for deployments that require that the user sign the request for enrollment by using a physical smart card for boot-strapping the enrollment process. The driver for the physical smart card does not need to be installed on the client machine as long as it is installed on the remote machine. This is made possible by smart card redirection functionality introduced in Windows Server 2003 that ensures that smart cards connected to the client computer are available for use in the remote session.

Alternatively, on a client computer, without establishing a remote desktop session, the user can also enroll for certificates from the certificate management console (certmgr.msc) or from within custom certificate enrollment applications that can create a request and submit to a server (for example, a Registration Authority) that has controlled access to the certification authority (CA). This will require specific enterprise configuration and deployments for Certificate Enrollment Policies (CEP) and Certificate Enrollment Services (CES).

##### Certificate lifecycle management

Certificate renewal can be done through remote desktop sessions or CEP/CES. Renewal requirements could be different from initial issuance requirements based upon renewal policy.

Certificate revocation requires careful planning. For cases when the information about the certificate to be revoked is reliably available, the specific certificate can be easily revoked. For cases when it is not easy to determine the certificate to be revoked (i.e. when the employee reports a lost/compromised device and information associating a device with a certificate is not available), all certificates issued to the user under the policy that was used for certificate issuance, may need to be revoked.

## Unmanaged cards

As the name suggests, an unmanaged virtual smart card is not serviceable by the IT administrator. It may be suitable for a deployment that does not have an elaborate smart card deployment management tool and using remote desktop connections to manage the card is not desirable. Since such cards are not serviceable by the IT administrator, for situations where the user needs help with their virtual cards (for example, PIN reset, PIN unblock etc.), the only option available to the user is to delete the card and create it again. Doing so will result in loss of credentials and will require the user to re-enroll.

### Card creation

A virtual smart card can be created by the user by using a built-in tool, Tpmvscmgr.exe, executed from a command prompt running with administrative privileges (elevated command prompt). The following command will create the unmanaged card that can be used for enrollment of certificates:

tpmvscmgr.exe create /name “VirtualSmartCardForCorpAccess” /AdminKey RANDOM /PIN PROMPT /generate

This command will create a card with a randomized administrator key. The key is discarded after the creation of the card automatically. This means that if the user forgets the PIN or wants to the change the PIN, the user will need to delete the card and create it again. To delete the card, the user can run the following command:

tpmvscmgr.exe destroy /instance <instance ID>

where <instance ID> is the value printed on the screen when the user creates the card (i.e. for the first card created instance id is ROOT\SMARTCARDREADER\0000).

##### Certificate issuance

Initial enrollment can be done through different ways depending upon security requirements unique to deployments. The user can also enroll for certificates from the certificate management console (certmgr.msc) or from within custom certificate enrollment applications that can create a request and submit to a server that has access to the Certificate Authority. This will require specific enterprise configurations and deployments for Certificate Enrollment Policies (CEP) and Certificate Enrollment Services (CES). Windows 8 has built-in tools (Certreq.exe and Certutil.exe) that can be used by scripts to perform the enrollment from the command line.

###### Requesting the certificate by providing domain credentials only

In its simplest form, a user can request a certificate by simply providing his or her domain credentials to request a certificate. This can be done through a script that can perform the enrollment through built-in components.

Alternatively, instead of a script, a modern application (as a LOB app) can be installed on the computer to perform enrollment by generating a request on the client and submitting it to an HTTP server that can then forward the request to a Registration Authority (RA).

Another option is to have the user access an enrollment portal available through Internet Explorer®. The webpage can use the scripting APIs to perform enrollment.

###### Signing the request with another certificate

A user can be provided with a short-lived certificate through a PFX file that the user can import into the MY store, which is the user’s certificate store. Then, a user can be offered a script that can sign the request with the short-lived certificate to request a virtual smart card. The PFX file can be generated for the user by initiating a request from a domain-joined computer and any additional policy constraints can be enforced on the PFX generation to assert the identity of the user.

For deployments that require the user to sign the request with a physical smart card (if physical smart cards are also issued to the user), the following could be done:

1. User initiates a request from the computer.
2. User then completes the request from a domain-joined computer by using the physical smart card to sign the request.
3. User then downloads the request to the smart card on the client computer.

###### Using one-time password for enrollment

 Another option to ensure that the user is authenticated strongly before a virtual smart card certificate is issued to the user is by sending the user a one-time password through SMS, email, or phone and then asking the user to type the one-time password during enrollment from an application or a script on the desktop that invokes built-in command-line utilities.

##### Certificate lifecycle management

Certificate renewal can be done from the same tools that are used for initial enrollment. CES and CEP can also be used to perform auto renewal.

Certificate revocation requires careful planning. For cases when the information about certificate to be revoked is reliably available, the specific certificate can be easily revoked. For cases when it is not easy to determine the certificate to be revoked ( i.e. when the employee reports a lost/compromised device and information associating a device with a certificate is not available), all certificates issued to the user under the policy that was used for certificate issuance, may need to be revoked.