*Research paper*

**Integration of smart cards in Windows 10**

**Leontina Hulaj1, Visar Berisha 2 Lundrim Rexhepi 3**

1 [leontina.hulaj@student.uni-pr.edu](mailto:leontina.hulaj@student.uni-pr.edu)

2 [visar.berisha1@student.uni-pr.edu](mailto:visar.berisha1@student.uni-pr.edu)

3 [lundrim.rexhepi1@uni-pr.edu](mailto:lundrim.rexhepi1@uni-pr.edu)

Received: 10 January 2021; Accepted: 10 January 2021;

**Abstract:** Authentication is a process for verifying the identity of an object or person. When you authenticate an object, such as a smart card, the goal is to verify that the object is genuine. When you authenticate a person, the goal is to verify that you are not dealing with an imposter.

In a networking context, authentication is the act of proving identity to a network application or resource. Typically, identity is proven by a cryptographic operation that uses a key only the user knows (such as with public key cryptography), or a shared key. The server side of the authentication exchange compares the signed data with a known cryptographic key to validate the authentication attempt. Storing the cryptographic keys in a secure central location makes the authentication process scalable and maintainable.

In this paper, we present smart cards, tamper-resistant portable storage devices that can enhance the security of tasks such as authenticating clients, signing code, securing e-mail, and signing in with a Windows domain account.

For smart cards, Windows supports a provider architecture that meets the secure authentication requirements and is extensible so that you can include custom credential providers.

Smart cards can be used to sign in to domain accounts only, not local accounts. When you use a password to sign in interactively to a domain account, Windows uses the Kerberos version 5 (v5) protocol for authentication. If you use a smart card, the operating system uses Kerberos v5 authentication with X.509 v3 certificates.

**Keywords:**  Smartcards, authentication, Kerberos, certificates,

1. **Introduction**

Administrators are increasingly aware of the dangers that result if they rely only on user names and passwords to provide authentication to network resources. Attackers can guess user names, or use such publicly available information as an e-mail address on a business card to identify a user name. When an attacker knows a user name, the only security mechanism that remains is a user’s password. Single secrets such as passwords can be effective security controls. A long password of more than 10 characters that consists of random letters, numbers, and special characters can be very difficult to crack.

A long password of more than 10 characters that consists of random letters, numbers, and special characters can be very difficult to crack. Unfortunately, users cannot always remember these sorts of passwords, partly due to fundamental human limitations. Research by George A Miller, published in The Psychological Review in 1956, concluded that the human brain has a short-term memory limit of between five and nine random characters, with an average of seven. However, most security guidance recommends at least an eight-character random password. Because most users cannot commit an eight character random password to memory, many opt to write it down on a piece of paper. Users rarely show great discretion when they write down passwords, and so provide opportunities for attackers to compromise their credentials. Where there are no restrictions on password complexity, users tend to choose easy to remember passwords such as "password" or other easily guessed words. Pass phrases are longer passwords that users can remember more easily.

Two-factor authentication systems overcome the issues of single secret authentication by the requirement of a second secret.

Two-factor authentication uses a combination of the following items:

* Something that the user has, such as a hardware token or a smart card.
* Something the user knows, such as a personal identification number (PIN).

Smart cards and their associated PINs are an increasingly popular, reliable, and cost effective form of two-factor authentication. With the right controls in place, the user must have the smart card and know the PIN to gain access to network resources.

Because administrator-level accounts have a wide range of user rights, compromise of one of these accounts can give an intruder access to all network resources. It is essential to safeguard administrator-level access because the theft of domain administrator-level account credentials jeopardizes the integrity of the domain, and possibly the entire forest, together with any other trusting forests.

Two-factor authentication is particularly important with remote users, because it is not possible to provide any form of physical access control for remote connections. Two-factor authentication with smart cards can increase security on the authentication process for remote users who connect through virtual private network (VPN) links.

**2. What are smart cards**

The term smart card has been used to describe a class of credit card-sized devices with varying capabilities: stored-value cards, contact-less cards, and integrated circuit cards (ICC). All of these cards differ in functionality from each other and from the more familiar magnetic-stripe cards used by standard credit, debit, and ATM cards. It is the ICC that is of most interest to the personal computer, and Windows, because it is able to perform more sophisticated operations such as digital signature and key exchange.

Smart cards are tamper-resistant portable storage devices that can enhance the security of tasks such as authenticating clients, signing code, securing e-mail, and signing in with a Windows domain account.

Smart cards provide:

* Tamper-resistant storage for protecting private keys and other forms of personal information.
* Isolation of security-critical computations that involve authentication, digital signatures, and key exchange from other parts of the computer. These computations are performed on the smart card.
* Portability of credentials and other private information between computers at work, home, or on the road.

Smart cards can be used to sign in to domain accounts only, not local accounts. When you use a password to sign in interactively to a domain account, Windows uses the Kerberos version 5 (v5) protocol for authentication. If you use a smart card, the operating system uses Kerberos v5 authentication with X.509 v3 certificates.

**2.1 Smart Card Architecture**

Authentication is a process for verifying the identity of an object or person. When you authenticate an object, such as a smart card, the goal is to verify that the object is genuine. When you authenticate a person, the goal is to verify that you are not dealing with an imposter.

In a networking context, authentication is the act of proving identity to a network application or resource. Typically, identity is proven by a cryptographic operation that uses a key only the user knows (such as with public key cryptography), or a shared key. The server side of the authentication exchange compares the signed data with a known cryptographic key to validate the authentication attempt. Storing the cryptographic keys in a secure central location makes the authentication process scalable and maintainable.

For smart cards, Windows supports a provider architecture that meets the secure authentication requirements and is extensible so that you can include custom credential providers. This topic includes information about:

* Credential provider architecture
* Smart card subsystem architecture

**2.1.1 Credential provider architecture**



Table 1. CREDENTIAL PROVIDER ARCHITECTURE

The table 1 lists the components that are included in the interactive sign-in architecture of the Windows Server and Windows operating systems.

Interactive sign-in in Windows begins when the user presses CTRL+ALT+DEL. The CTRL+ALT+DEL key combination is called a secure attention sequence (SAS). To keep other programs and processes from using it, Winlogon registers this sequence during the boot process.

After receiving the SAS, the UI then generates the sign-in tile from the information received from the registered credential providers. The following graphic shows the architecture for credential providers in the Windows operating system.

2.1.2 Smart card subsystem architecture

Vendors provide smart cards and smart card readers, and in many cases the vendors are different for the smart card and the smart card reader. Drivers for smart card readers are written to the Personal Computer/Smart Card (PC/SC) standard. Each smart card must have a Cryptographic Service Provider (CSP) that uses the CryptoAPI interfaces to enable cryptographic operations, and the WinSCard APIs to enable communications with smart card hardware.

2.2 Smart card sign-in flow in Windows

Most issues during authentication occur because of session behavior changes. When changes occur, the Local Security Authority (LSA) does not reacquire the session context; it relies instead on the Cryptographic Service Provider to handle the session change.

In the supported versions of Windows designated in the Applies To list at the beginning of this topic, client certificates that do not contain a UPN in the subjectAltName (SAN) field of the certificate can be enabled for sign-in, which supports a wider variety of certificates and supports multiple sign-in certificates on the same card.

Support for multiple certificates on the same card is enabled by default. New certificate types must be enabled through Group Policy.

If you enable the Allow signature keys valid for Logon credential provider policy, any certificates that are available on the smart card with a signature-only key are listed on the sign-in screen. This allows users to select their sign-in experience. If the policy is disabled or not configured, smart card signature-key-based certificates are not listed on the sign-in screen.

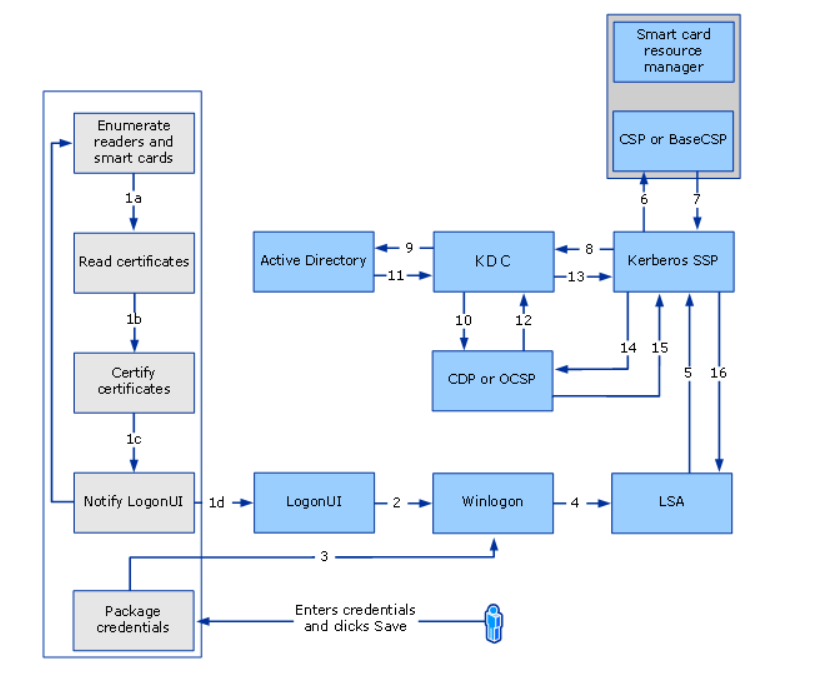


Figure 1.Smart card sign-in flow

The figure 1 illustrates how smart card sign-in works in the supported versions of Windows.

1. **ACTIVE DIRECTORY AND KERBEROS CONCEPTS**

The following concepts are important to understanding how smart card logon works in Windows 10

**3.1 Kerberos**

The Kerberos authentication protocol provides a mechanism for mutual authentication between a client and a server, or between different servers. One benefit of mutual authentication using the Kerberos version 5 protocol is that trust between security authorities for Windows 10 domains is by default two-way and transitive. The Kerberos version 5 protocol relies heavily on an authentication technique involving shared secrets. The basic concept is quite simple: If a secret is known by only two people, then either person can verify the identity of the other by confirming that the other person knows the secret. Rather than sharing a password, communication partners share a cryptographic key, and they use knowledge of this key to verify one another’s identity. For the technique to work, the shared key must be symmetric—a single key must be capable of both encryption and decryption. One party proves knowledge of the key by encrypting a piece of information, the other by decrypting it.

**3.2 PKINIT**

There is an extension to the Kerberos version 5 protocol proposed by the IETF called PKINIT that allows for the use of a public key certificate in place of a password during the initial authentication. The PKINIT extension is the basis for smart card logon support in Windows 10 and does not change the requirement for a long-term symmetric key. Rather, the public key in the certificate is used to encrypt a symmetric key returned as a result of a successful authentication that then must be decrypted using the associated private key stored on the smart card.

**3.3 Key Distribution Center**

Windows 10 implements the Key Distribution Center (KDC) as a domain service and uses the domain’s Active Directory as its account database. The KDC is a single process comprised of two services: the Authentication Service (AS) and the Ticket-Granting Service (TGS). The AS issues Ticket Granting Tickets (TGTs) to authenticated principals (that is, users, machines, services) for admission to the TGS. The TGS issues tickets for admission to other services in the domain or to a TGS in another trusted domain. Each domain controller has a KDC that runs in the process space of the Local Security Authority (LSA). Any domain controller can accept authentication requests and ticket-granting requests addressed to the domain’s KDC.

**3.4 Active Directory**

The Active Directory is primarily a namespace that is a bounded area in which a given name can be resolved. Name resolution is the process of translating a name into some object or information that the name represents. A telephone directory forms a namespace in which the names of telephone subscribers can be resolved to telephone numbers. The Active Directory forms a namespace in which the name of an object in the directory can be resolved to the object itself. An object is a distinct, named set of attributes that represents something concrete such as a user, a printer, or an application. The attributes hold data describing the subject that is identified by the directory object. Attributes of a user might include the user’s common name, a certificate, or an e-mail address. All Active Directory objects are protected by an Access Control List (ACL). ACLs determine who can see the object and what actions each user can perform on the object. The existence of an object is never revealed to a user who is not allowed to see it.

**3.5 Domains, Forests and Trust**

A domain is a single security boundary in Windows 10. Active Directory is comprised of one or more domains. On a stand-alone computer, the domain is the computer itself. A domain can span more than one physical location. Every domain has its own security policies and security relationships with other domains. When multiple domains are connected by trust relationships and share a common schema, configuration, and global catalog, you have a domain tree. Multiple domain trees can be connected together into a forest. A forest is a set of one or more trees that do not form a contiguous namespace. All trees in a forest share a common schema, configuration, and Global Catalog. All trees in a given forest trust each other via transitive, hierarchical Kerberos trust relationships. Unlike a tree, a forest does not need a distinct name. A forest exists as a set of cross-reference objects and Kerberos trust relationships known to the member trees. Trees in a forest form a hierarchy for the purposes of Kerberos trust; the tree name at the root of the trust tree can be used to refer to a given forest Kerberos uses the Active Directory as its account database from which it obtains information about security principals. When a domain is joined to a Windows 10 domain tree, a Kerberos trust relationship is automatically established between the joined-from domain and its parent in the tree. Kerberos trust is transitive, so no additional trust relationships are required among tree members. The trust hierarchy is stored in cross-reference objects in the directory. Each domain controller keeps a writeable copy of the directory so that accounts can be created, passwords reset, and group membership modified on any domain controller. Changes made to one replica of the directory are automatically propagated to other replicas. Windows 10 does not, however, implement the Kerberos replication protocol. Instead it replicates the information store for Active Directory using a multi-master protocol over a secure channel established between replication partners.

**4. Implementation Prerequisites**

Smart card deployment requires a planned approach to ensure that organizations consider all the issues before the start of the implementation phase. This section covers the most common prerequisites, although there might be additional requirements in your environment.

**4.1 Identification of Accounts**

The identification of the users and the groups that require smart card access is an important part of a smart card deployment.

Note: Organizations that have the budget and security requirements to implement smart card access for all users can skip this step.

Groups and users that require smart cards might include:

* Domain administrators for all domains in the forest
* Schema administrators
* Enterprise administrators
* Database administrators
* Human resource administrators
* Users who have remote access
* Users who have either user or administrative access to sensitive resources, such as accounting and finance information

An organization might also require smart card access for users and groups not in the previous list, such as board-level personnel. The identification of these accounts early in the process helps define the scope of the project and control costs. To identify critical accounts, you must define when to use smart cards. For example, good security practice recommends that administrators have two user accounts: a standard account for daily tasks such as e-mail, and an administrator-level account for server maintenance and other administrative tasks. Usually, the administrator would log on with the user-level account, and use the Secondary Logon service to perform administrative tasks. Alternatively, the administrator can use the Remote Desktop for Administration component of Windows Server 2003, which supports smart card logon.

**4.2 Smart Card Infrastructure Support**

Smart cards require a suitable infrastructure with support from the operating system and network elements.

Microsoft provides support for smart card implementations that use the following components:

* Microsoft Certificate Services or external Public Key Infrastructure (PKI)
* Certificate templates
* Windows Server 2003
* The Active Directory® directory service
* Security Groups
* Group Policy
* Enrollment Stations and Enrollment Agents
* Activation Web Server
* Extensible Authentication Protocol – Transport Layer Security (EAP – TLS) — required for remote access solutions only Additional components include enrollment stations and enrollment agents.

**4.3 Public Key Infrastructure**

Smart cards require a PKI to provide certificates with public key/private key pairs that enable account mapping in Active Directory. You can implement this PKI in one of two ways: provision the internal certificate infrastructure to an external organization or use Certificate Services in Windows Server 2003. Organizations can outsource all or part of the certificate management process for smart cards. Financial organizations can benefit if they link their PKI to an external trusted root for e-mail verification and for secure transactions with partner organizations. An alternate approach is to use Certificate Services in Windows Server 2003 to provide the PKI.

The PKI must have a mechanism that deals with certificate revocation. Certificate revocation is necessary when a certificate expires or when an attacker could have compromised a certificate. Each certificate includes the location of its certificate revocation list (CRL).

**4.4 Certificate Templates**

Windows Server 2003 provides specific certificate templates to issue digital certificates for use in smart cards. You can copy and customize these certificates to fit your organization's requirements.

The three certificate templates for smart card use are:

* Enrollment Agent. Allows an authorized user to request certificates for other users.
* Smartcard User. Lets a user log on with a smart card and sign e-mail. Also provides client authentication.
* Smartcard Logon. Enables a user to log on with a smart card and provides client authentication but does not enable signed e-mail. Windows Server 2003, Enterprise Edition, provides version 2 (v2) templates that you can modify and extend to provide multiple capabilities such as logon, signed e-mail messages, and file encryption. You can also extend certificate templates to provide additional information that your organization requires, such as medical details or pension entitlements. Windows Server 2003, Enterprise Edition supports autoenrollment, which makes management of smart cards easier in a large organization. The certificate renewal request can use the current certificate to sign the request.

**4.5 Security Groups**

The smart card deployment and management process is significantly easier if you use security groups within Active Directory to organize users. For example, a typical smart card deployment might require you to create the following security groups:

* Smart card enrollment agents. Smart card enrollment agents are responsible for distribution of smart cards to users. The next section covers enrollment agents in detail.
* Smart card staging. The smart card staging group contains all users who are authorized to receive smart cards, but for whom an enrollment agent has not yet enrolled and activated their cards.
* Smart card users. This group contains all users who have completed the enrollment process and have an activated smart card. The enrollment agent moves the user from the smart card staging group to the smart card users group.

**4.6 Group Policy Group**

Policy enables you to apply configuration settings to multiple computers. You can set up the requirement to use smart cards for interactive logon in a Group Policy object (GPO) and then apply that GPO to organizational units or sites in Active Directory.

**4.7 Activation Web Server**

An activation Web server is custom component that enables users to activate their new smart cards by PIN reset. Some vendor software development kits (SDKs) provide tools to assist in the construction of an activation Web server. Microsoft does not provide the activation server component. To reset the PIN, the user runs a cryptographic service provider (CSP) utility that generates a hexadecimal challenge string from the smart card. The user enters this challenge string into a field on the Web page and the activation Web server generates a response. The user types the response into the response field in the utility, which then allows the user to set the smart card PIN. The activation Web server can also be part of the management process. Help desk operators can use this process to unblock cards where the user has entered the incorrect PIN too many times. In this case, the user reads the challenge to the help desk operator, who replies with the response.

**4.8 Evaluating Smart Cards**

The primary factor during the evaluation of smart cards is to ensure that the model you choose can support your planned key length. Windows Server 2003 supports certificate key lengths from 384 bits (low security) to 16,384 bits (maximum security). Certificates that have longer key lengths provide greater security than shorter key lengths, but longer key lengths significantly increase the time to log on with a smart card. Memory limitations in the smart card also restrict the maximum key length you can use. Certificate key lengths of 1,024 bits are suitable to secure administrator accounts or to secure remote access.

A certificate with a 1,024-bit key takes approximately 2.5 KB of memory space in the smart card. Other memory requirements include the operating system (16 KB), smart card vendor applications such as the CSP (8 KB), and the smart card file and directory structure (4 KB). Hence, smart cards that have less than 32 KB of memory are unlikely to be suitable for the storage of logon certificates and provide the required functionality to extend a smart card solution. The second factor to consider is whether the card has built-in support for Windows Server 2003 and Windows XP. Before you purchase smart cards, discuss your requirements with the vendor.

1. **How Smart card authentication works**

A smart card can be used to authenticate to a Windows 10 domain in three ways. The first is interactive logon involving Active Directory, the Kerberos version 5 protocol, and public key certificates. The second is client authentication where a user is authenticated using a public key certificate that matches an account stored in Active Directory. The third is remote logon that uses a public key certificate with the Extensible Authentication Protocol (EAP) and Transport Layer Security (TLS) to authenticate a remote user to an account stored in Active Directory.

**5.1 Interactive Logon**

Interactive Logon using a smart card begins when a user inserts a smart card into a smart card reader that signals the Windows 10 operating system to prompt for a Personal Identification Number (PIN) instead of a username, domain name and password. The card insertion event is equivalent to the familiar Ctrl-Alt-Del secure attention sequence used to initiate a password-based logon. However, the PIN the user provides to the logon dialog is used to authenticate only to the smart card and not to the domain itself. A public key certificate stored on the smart card is used to authenticate to the domain using the Kerberos version 5 protocol and its associated PKINIT extension.

**5.2 Logon Request**

After a user inputs a PIN to the logon dialog, the operating system begins a sequence of actions to determine whether the user can be identified and authenticated based on credential information the user has provided (PIN and smart card). The logon request first goes to the LSA that subsequently forwards it to the Kerberos authentication package running on the client. The Kerberos package sends an authentication service (AS) request to the KDC service running on a domain controller to request authentication and a Ticket Granting Ticket (TGT). As part of the AS request, the client-side Kerberos package includes the user’s X.509 version 3 certificate, retrieved from the smart card, in the pre-authentication data fields of the AS request. An authenticator, included in the pre-authentication data fields, is digitally signed by the user’s private key so that the KDC can verify the AS request originated from the owner of the accompanying certificate.

**5.3 Certificate Verification**

Before the KDC can satisfy the AS request, it must first verify the certification path of the user’s certificate to ensure that it can be trusted. The KDC uses CryptoAPI to build a certification path from the user’s certificate to a root CA certificate residing in the system root store. If the KDC fails to build a valid certificate chain for any reason (that is, root certificate is not trusted, cannot find parent certificates, revocation status cannot be determined) the KDC will return an error and fail the request. The KDC must also verify that the issuing CA is authorized to issue certificates whose name information can be used as a basis for authentication within the domain. In Windows 10, the issuing CA must be an enterprise CA published in the Active Directory in order to be trusted for authentication. This is required in order to prevent a rogue CA, trusted under one CA hierarchy, from issuing certificates into another domain’s namespace. While this type of attack is extremely difficult and depends on the rogue CA obtaining issuance rights from a legitimate parent CA, the solution to require an enterprise CA published in Active Directory was implemented to remove the potential for an attack.

**5.4 Digital Signature Verification**

Upon successful verification of the user’s certificate, the KDC then uses CryptoAPI to verify the digital signature on the authenticator that was included as signed data in the pre-authentication data fields. The signature verification is done using the public key from the user’s certificate to prove that the request originated from the owner of the public key. Because the certificate was retrieved from the smart card and the authenticator was signed using the private key stored in the smart card, the digital signature must be legitimate because the user had to authenticate to the smart card in order for the private key to sign the authenticator. After verifying the signature, the KDC service must then validate the timestamp in the authenticator to ensure the request is not a replay attack.

**5.5 Account Lookup and TGT**

Upon verifying that a user is who they say they are and that the certificate can be used to authenticate to the domain, the KDC service then queries the domain’s directory for account information. The KDC service retrieves user account information from Active Directory based on the User Principal Name (UPN) specified in the Subject Alternative Name field in the user’s public key certificate. The account information that the KDC retrieves from the directory is used to construct a TGT. The TGT will include the user’s Security ID (SID), the SIDs for any domain groups to which the user belongs, and potentially the SIDs for any universal groups in which the user is a member (in a multi-domain environment). The list of SIDs is included in the TGT’s authorization data fields. The KDC encrypts the TGT using a random key generated specifically for this purpose. The random key is itself encrypted using the public key from the user’s certificate and the encrypted key is included in the pre-authentication data field of the KDC’s response. The KDC signs the reply using its private key so that the client can verify the reply is from a trusted KDC. The client verifies the KDC’s signature by first building a certification path from the KDC’s certificate to a trusted root CA and then using the KDC’s public key to verify the reply signature. The KDC also signs the TGT’s authorization data using the server’s key that is then signed with the KDC’s secret key so that a rogue service cannot alter the authorization data after the TGT has been issued. The client, upon receipt of the KDC’s response, will extract the encrypted random key, decrypt it, and use the resulting key to decrypt the TGT. Once in possession of the TGT, the standard Kerberos version 5 protocol is used to request tickets from the TGS for other domain resources. It should be noted that supplemental credentials are generated as part of a Kerberos logon so that access to down-level servers such as those running the Windows NT® 4.0operating system will still work. This is true even if the user has never used a password on the computer. When an account is created a one-way function (is generated and added as an attribute of the account for use as a supplemental credential for down-level authentication.

**5.6 Offline Logon**

When a user is disconnected from the network or the domain controller is unreachable due to failure somewhere along the network path, a user must still be able to logon to his or her computer. With passwords this capability is supported by comparing the hashed password stored by the LSA with a hash of the credential that the user supplied to the GINA during logon. If the hashes are the same then the user can be authenticated to the local machine. In the smart card case, offline logon requires the user’s private key to decrypt supplemental credentials originally encrypted using the user’s public key. If the user has multiple smart cards then the supplemental credentials must be encrypted and referenced based on the hash of the certificate to ensure that the user can perform an offline logon regardless of what card is used.

**5.7 Client Authentication**

Because smart card support is integrated with CryptoAPI, the Secure Sockets Layer (SSL) and the Transport Layer Security (TLS) protocols do not need to know anything about a smart card in order for smart cards to work with these protocols. The role of the smart card in client authentication is to sign a part of the protocol during the initial SSL session negotiation. Because the private key corresponding to the public key certificate is stored on the smart card, the method of authentication is stronger because use of the private key requires the holder of the card to authenticate to the card and to the domain. In addition, the private key operation performed during the initial session negotiation is performed on the card such that the private key is never exposed to the host computer or network.

**5.8 Mutual Authentication**

Both the SSL 3.0 and TLS 1.0 protocols support mutual authentication meaning the client can authenticate the server and the server can authenticate the client. Server authentication is when the client authenticates the server by verifying the cryptographic signatures on the server’s certificate, and any intermediate CA certificates, to a root CA certificate residing in the trusted root store on the client. Authentication of the client by the server is accomplished in the reverse manner as server authentication. The server verifies the cryptographic signatures on the client’s certificate, and any intermediate CA certificates, to a root CA installed in the trusted root store on the server. Once the identity of the client is verified, the server needs to establish a security context with appropriate authorization that determines what resources the client is allowed to use on the server.

**5.9 Authorization**

Public-key client authentication in Windows 10 uses information in the client’s certificate to map to domain access control information. Windows 10 implements a security service that uses certificate information to map to accounts stored in the Active Directory for the purpose of determining access rights for the authenticated client. This directory operation can be performed based on the UPN in the certificate or by searching the directory for an account that matches properties, issuer or issuer and subject, in the client certificate. When an SSL or TLS session is established, the secure channel provider first attempts to find a user account in the domain’s directory based on the UPN in the certificate. The UPN is included in the certificate in the Alternative Subject Name field and specifies the exact user account name (prefix) and the domain name (suffix) where the account is located. Just as in Kerberos-based smart card logon, the issuing CA must be authorized to issue certificates for the domain whose name information can be trusted for identification and authentication. If there is no UPN match, or the issuing CA is not authorized to issue certificates for domain authentication, the provider then attempts to query the directory to find an account whose Alternate Security Identities attribute contains an explicit mapping to the client certificate. An explicit mapping between a certificate and a user account requires an administrator to perform an action to create the mapping. The mapping to the client certificate can be based on either the issuer name or the issuer and subject names in the certificate. An account can have one or more certificates associated with it to facilitate using one account for multiple external users. A certificate cannot be mapped to multiple accounts stored in the domain’s directory. Authentication will fail if a certificate is mapped to more than one account.

**5.10 Remote Access**

Support for extensible authentication for remote users is supported in Windows 10 by the remote access service (RAS). The remote access server supports EAP to allow vendor-supplied authentication modules to be added support for a variety of authentication methods ranging from smart card to one-time passwords to biometrics. Windows 10 includes a built-in module for smart cards to enable strong authentication for remote users. A remote logon actually involves two separate authentications: one to the RAS server and the other to the network. The first authentication results in the RAS server being authenticated by the client and establishment of a connection between the client and server. As a result of this connection, some RAS-specific policies and account attributes are applied to the client. Account attributes are applied on a per user basis and include properties such as access rights, callback options, static routes, and so forth. RAS policies are specific to how the server should interact with the client and are rules-based. This allows for management of users by matching on the properties of the connection, group membership, profile, and so forth.

1. **DEPLOYING SMART CARDS**

The value to a corporation deploying smart cards is increased network security through stronger authentication methods. Windows 10 makes it possible to deploy strong authentication using smart cards by leveraging operating system features such as Kerberos, Active Directory, and the variety of administrative tools used to manage a public key infrastructure. Windows 10 Professional, Windows 10 Server and Windows 10 Advanced Server have integrated smart card and public key technologies to enable corporations to take immediate advantage of them in a cost-effective manner without the need to outsource certificate management or purchase expensive and proprietary application plug-ins. For any business considering deployment of smart cards, there are some basic questions that must be answered first.

Here are four simple questions to consider when planning a smart card deployment:

* Which user populations should be required to use smart cards?
* What policies and procedures should be established to manage the cards and certificates?
* How should smart cards be issued to users?
* What smart card hardware is available and compatible with Windows 10?

**6.1 Who Should Use Smart Cards?**

It is recommended that users who do not perform advanced tasks such as joining computers to domains or promoting servers to domain controllers be issued smart cards and not passwords. This category of user should represent a significant portion of a company’s employee population. These users could be professional workers, suppliers, contractors, or anyone else who is not trusted to administer a computer or the network. Windows 10 supports organizing users based on their roles within a domain and defines three distinct categories: Administrator, Power User and User. Administrators are all-powerful. The default Windows 10 security settings do not restrict Administrative access to any registry or file system object. Administrators can perform any and all functions supported by the operating system. Any right that the Administrator does not have by default, they can grant to themselves. Power Users are less powerful than administrators but are still able to install applications, configure system settings, and so forth. The default Windows 10 security settings for Power Users are backward compatible with the default security settings for users in the Windows NT 4.0 operating system. Users are the opposite of administrators. The default security settings are designed to prohibit Users from compromising the integrity of the operating system and installed applications if Windows 10 is clean-installed on an NTFS partition. Users cannot modify machine-wide registry settings, operating system files, or program files. Users cannot install applications that can be run by other Users (preventing Trojan horses). Users cannot access other users’ private data. Members of the Users group should use smart cards for authentication because their role within the enterprise should not require them to perform advanced tasks. This group of users should represent a significant portion within any corporation, making smart card deployment a worthwhile investment because managing passwords for this population will no longer be necessary. Because the smart card can also be used to authenticate over SSL, in addition to interactive and remote access logon, the value of deploying smart cards is high because large populations of users can migrated away from passwords that have proven difficult to manage.

However, it is not feasible to recommend that Power Users or Administrators use smart cards exclusively since they may have a need to perform operations that involve a secondary authentication requiring a username, domain name and password. In particular, smart card-based authentication cannot be used in the following scenarios:

* The user is required to join his or her computer to a domain.
* The user must perform administrative tasks such as promote a server to be a domain controller.
* The user needs to configure a network connection for remote access.

**6.2 What Policies Are Needed?**

Public key security policy is one aspect of security policy and is integrated with the Windows 10 policy management infrastructure to provide a consistent model for administering public key policy alongside policies for other services. There are several types of policy that can be set to control the use of smart cards within a Windows 10 domain.

**6.3 Smart Card Required**

Windows 10 supports a per user account policy, smart card required for interactive logon, that requires a smart card to effect an interactive logon. What this means is that once the policy is set on an account, the user cannot use a password to log on to the account, interactively or from a command-line. The policy applies to interactive and network logon only, but not to remote access logon which uses a different policy configured on the remote access server. While setting the smart card required for interactive logon policy on an account is not recommended for every user in an enterprise, it should be set for those users who are members of the Users group that are using smart cards to log on to a Windows 10 domain.

* The smart card required for interactive logon policy is not recommended for the following scenarios:
* The user is required to join his or her computer to a domain.
* The user must perform administrative tasks such as promote a server to be a domain controller.
* The user needs to configure a network connection for remote access.

In each of these scenarios, the user will need to provide a username, domain name and password because these tasks do not support using public key-based authentication. In future releases, Windows 10 will support the use of public key certificates for authentication in those scenarios.

**6.4 On Smart Card Removal**

When a user walks away from a computer with an active logon session, he or she is expected to either logoff or lock the computer. If the user fails to secure the computer, the screensaver program could lock the computer if it is configured to do so. Otherwise the computer is open for an attack by a malicious insider who can do various things such as send unfriendly email as the logged on user. The on smart card removal policy is a local computer policy administered on a per machine basis on not on a per user account basis like the smart card required for interactive logon policy. The decision to set the on smart card removal policy depends on the needs of the corporation and how users interact with computers. In situations where users interact with computers in an open floor or kiosk environment, the use of such a policy is highly recommended. In situations where users have a dedicated computer or multiple computers that only they use, it may not be necessary to set this policy if other means of locking the computer are enabled such as a screensaver program. As with many security policy decisions, the trade-off is increased security versus usability.

**6.5 Personal Identification Numbers**

While passwords are inherently weak, and are made weaker by users choosing easy-to-remember pass-phrases, smart card PINs do not have to follow the same rules as "strong passwords" because the cards are not open to classic dictionary attacks. An easy-to-remember PIN is not a problem because a smart card will lock when too many wrong PIN inputs are attempted in a row. Since the PIN itself is never transmitted over-the-network in any form, a replay attack is extremely difficult because it also requires possession of the physical card as opposed to a sniff of a network packet as in a password-based attack.

**6.6 How Should Smart Cards Be Issued?**

Because a smart card is a trusted ID like an employee badge, most corporations will want to integrate smart cards with the employee badge rather than issue a second ID which must be managed separately. Obtaining a badge typically requires a visit to a security office where the employee must prove identity and then have his or her picture taken to create the badge used to gain access to a building or facility. The only delta to the above procedure is the badge would now also contain a certificate issued to the employee by the corporation.

No matter how a corporation chooses to deploy smart cards, the decision to integrate with the employee badge or not should be based on business needs that must balance the need for increased security with overall usability across the employee population.

1. **Advantages & Disavantages**

**7.1 Advantages**

* Flexibility

There is no need, for example, to carry several cards: one card can simultaneously be an ID, a credit card, a stored-value cash card, and a repository of personal information such as telephone numbers or medical history. Such a card can be easily replaced if lost, and, because a PIN number (or other form of security) must be used to access information, is totally useless to people other than its legal bearer. At the first attempt to use it illegally, the card would be deactivated by the card reader itself.

* **More Secure**

Smart card readers are more secure than their counterparts as they use encryption and authentication technology. This is more secure than previous methods associated with payment cards.

* **Adaptable**

Smart card readers can be plugged into machines using a USB supported system, which can operate seamlessly with sales and inventory software. They also allow an easier time tracking customer purchases if you’re interested in starting a loyalty program. Smart credit card readers can be linked to customer databases to do research on customer purchases and help figure out what items are the most popular in sales.

**7.2 Disavantages**

* **Slow Adoption And Cost**

Not every store or restaurant has the hardware to use these cards, and the readers are more expensive due to the added security. Of course, this should change over time as more and more businesses make the switch.

* **Security Concerns**

Because the smart card is so new, Americans have been slow to trust them. These devices store a vast amount of sensitive information, which some people see as a security risk. However, as previously mentioned, evidence has shown that they are more secure than traditional cards.

1. **Conclusion**

The implementation of smart cards to authenticate remote access connections provides greater security than simple user name and password combinations. Smart cards implement two-factor authentication through a combination of the smart card and a PIN. Two-factor authentication is significantly more difficult to compromise and the PIN is easier for a user to remember than a strong password. The provision of smart card authentication for remote access users is a reliable and cost effective method that increases network security. This guide has taken you through the steps required to plan and implement this solution.

Smart cards of the future may even take on other forms and factors that will make them remarkably convenient to the user. Shortly, all PC’s and Network Computers will be integrated with smart card readers for both personal and private use. As technology advances there’s almost no limited that cannot be built into a common access card.

Reference

<https://docs.microsoft.com/en-us/windows/security/identity-protection/smart-cards/smart-card-architecture>

<http://www.itsecure.hu/library/file/Biztons%C3%A1gi%20%C3%BAtmutat%C3%B3k/Egy%C3%A9b%20biztons%C3%A1gi%20%C3%BAtmutat%C3%B3k/The%20Secure%20Access%20Using%20Smart%20Cards%20Planning%20Guide.pdf>

<https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/access-control>

http://tnlandforms.us/cns04/sclogonwp.pdf

Title of Site. Available online: URL (accessed on Day Month Year).

[1] About smart cards: Introduction. Available online: https://www.securetechalliance.org/smart-cards-intro-primer/#:~:text=A%20smart%20card%20is%20a,remote%20contactless%20radio%20frequency%20interface. (accessed on 09 Jan 21).

[2] Smart cards: Technical reference. Available online: https://docs.microsoft.com/en-us/windows/security/identity-protection/smart-cards/smart-card-windows-smart-card-technical-reference. (accessed on 10 Jan 21).