| Ch13 Key Terms | |
|---|---|
| AD CS | (Active Directory Certificate Services) Server role available in Windows Server 2008 that enables administrators to create and administer PKI certificates for users, computers, and applications. |
| autoenrollment | PKI feature supported by Windows Server 2003 and later that allows users and computers to automatically enroll for certificates based on one or more certificate templates, as well as use Group Policy settings in Active Directory. |
| Automatic Certificate Request | Public Key Policies setting that enables computers to automatically submit a request for a certificate from an Enterprise Certification Authority (CA) and install that certificate. |
| certificate | Digital document that contains identifying information about a particular user, computer, service, and so forth. The digital certificate contains the certificate holder's name and public key, the digital signature of the Certificate Authority that issued the certificate, as well as the certificate's expiration date. Also known as a digital certificate. |
| CPS | (Certificate Practice Statement) Provides a detailed explanation of how a particular Certification Authority manages certificates and keys. |
| Certificate Request Wizard | Enables a user to manually create a certificate request file by using the Certificates MMC snap-in. This wizard creates a request file that can be used by the Certification Authority MMC to generate a certificate based on the request. |
| CRL | (Certificate Revocation List) List that identifies certificates that have been revoked or terminated as well as the corresponding user, computer, or service. |
| Certificate Services Client–Auto-Enrollment | Public Key Policies setting that allows an administrator to enable or disable the automatic enrollment of computer and user certificates, in addition to renewing and requesting certificates based on certificate templates. |
| certificate template | Templates used by a CA to simplify the administration and issuance of digital certificates. |
| CA | (certification authority) Entity that issues digital certificates used by companies to sign SMTP messages exchanged between domain controllers, thereby ensuring the authenticity of directory updates. |
| Certification Authority Web Enrollment | Enables users to manually request certificates using a Web interface, located by default at https://<CA Name/certsrv on a CA that is running the Certification Authority Web Enrollment role service. |
| certutil | Extremely flexible command-line utility for administering Active Directory Certificate Services. |
| digital certificate | Digital document that contains identifying information about a particular user, computer, service, and so forth. The digital certificate contains the certificate holder's name and public key, the digital signature of the Certificate Authority that issued the certificate, as well as the certificate's expiration date. Also known as a certificate. |
| digital signature | Electronic signature (created by a mathematical equation) that proves the identity of the entity that has signed a particular document. |
| EFS | (Encrypting File System) Public Key Policies setting that enables an administrator to modify the list of recovery agents by adding other accounts as recovery agents. This setting is only available in the Computer Configuration node. |
| enrollment agent | Certificate generated by the enterprise CA that is used to generate a smart card logon certificate for users in the organization. |
| enterprise CA | Entity that can issue certificates only to users and computers in its own forest. |
| Enterprise Trust | Public Keys Policies setting that allows an administrator to define and distribute a certificate trust list (CTL) for external root certificate authorities (CAs). A CTL is a list of root CAs that the administrator has deemed to be reputable sources. |

| | |
|---|---|
| hierarchical | Arranged in a ranking system whereby many subordinate Cas within an organization can chain upward to a single root CA. |
| intermediate CA | In a hierarchy of certification authorities (CA), a single root CA issues certificates to several of these certification authorities. |
| issuing CA | Certification authority (CA) that issues certificates to users or computers. |
| key archival | Process by which private keys are maintained by the certification authority (CA) for retrieval by a recovery agent, if at all. |
| key recovery agent | User accounts that are configured with a Key Recovery Agent certificate that allows them to restore an escrow copy of a private key. |
| NDES | (Network Device Enrollment Service) Allows devices, such as hardware-based routers and other network devices and appliances, to enroll for certificates within a Windows Server 2008 PKI that might not otherwise be able to do so. |
| OCSP Response Signing certificate | Template that enables digital signatures, which are required for Online Certificate Status Protocol (OCSP) transactions. The template is located on any CA that will be used as an Online Responder. |
| OCSP | (Online Certificate Status Protocol) Protocol used by the Online Responder to respond to queries from clients requesting data about the status of a PKI certificate that has been issued by a particular CA. |
| Online Responder | Service that responds to requests from clients concerning the revocation status of a particular certificate, returning a digitally signed response indicating the certificate's current status. |
| principle of least privilege | Security best practice dictating that users should receive only the minimum amount of privileges needed to perform a particular task. |
| private key | Piece of information, used as part of the public key infrastructure (PKI), that is known only to the individual user or computer. |
| public key | Piece of information, used as part of the public key infrastructure (PKI). |
| public key cryptography | Mathematical algorithm utilizing public keys and private keys that is used by public key infrastructure (PKI) to communicate securely. |
| PKI | (public key infrastructure) System of digital certificates, certification authorities (CAs), and other registration authorities (RAs) that verify and authenticate the validity of each party involved in an electronic transaction using public key cryptography. |
| Public Key Policies | Area of Group Policy that offers greater administrative control in establishing rules and governing the issuance, maintenance, and guidelines within a public key infrastructure (PKI). |
| recovery agent | Configured within a CA to allow one or more users (typically administrators) to recover private keys for users, computers, or services if their keys are lost. |
| Responder array | Multiple Online Responders linked together to process status requests. |
| restricted enrollment agent | Limits the permissions required for an enrollment agent to configure smart cards on behalf of other users. |
| root CA | In a hierarchy of certification authorities (CA), this CA issues certificates to several intermediate CAs. |
| self-enrollment | Feature that enables users to request their own PKI certificates, typically through a Web browser. |
| shared secret key | Secret piece of information shared between two parties prior to being able to communicate securely. |
| signed | Certifies that the document originated from the person or entity in question. In cases where a digital signature is used to sign something, such as an email message, a digital signature also indicates that the message is authentic and has not been tampered with since it left the sender's Outbox. |
| SCEP | (Simple Certificate Enrollment Protocol) Network protocol that allows network devices to enroll for PKI certificates. |

| | |
|---|---|
| smart card | Small physical device, usually the size of a credit card or keychain fob, that has a digital certificate installed. Used with a PIN to enable logon to a secure resource. |
| smart card enrollment station | Dedicated workstation from which an administrator or another authorized user can preconfigure certificates and smart cards on behalf of a user or workstation. |
| smart card reader | Physical device attached to a workstation that enables users to utilize a smart card to authenticate to an Active Directory domain, access a Website, or authenticate to other secured resources. |
| standalone CA | Entity that can issue certificates only to users and computers in its own forest. Standalone CAs are not integrated with Active Directory. |
| subordinate CA | CA within an organization that chains upward to a single root CA that is authoritative for all certificate services within a given network. |
| Trusted Root Certification Authorities | Public Key Policies setting that determines whether users can choose to trust root CAs and the criteria that must be met by the CA to fulfill user requests. |
| two-factor authentication | Authentication method that requires a smart card and a PIN to provide more secure access to company resources. |
| Web enrollment | Feature that enables users to connect to a Windows Server 2008 CA through a Web browser to request certificates and obtain an up-to-date Certificate Revocation List. |