[MS-GLOS]:
Windows Protocols Master Glossary

Revision Summary

Date	Revision History	Revision Class	Comments
03/02/2007	0.1		MCPP Milestone 2
04/03/2007	1.0		Monthly release
05/11/2007	1.1		Monthly release
06/01/2007	1.1.1	Editorial	Revised and edited the technical content.
07/03/2007	1.1.2	Editorial	Revised and edited the technical content.

Date	Revision History	Revision Class	Comments
07/20/2007	1.1.3	Editorial	Revised and edited the technical content.
08/10/2007	1.1.4	Editorial	Revised and edited the technical content.
09/28/2007	1.1.5	Editorial	Revised and edited the technical content.
10/23/2007	1.1.6	Editorial	Revised and edited the technical content.
11/30/2007	1.2	Minor	Updates to some terms.
01/25/2008	1.3	Minor	Updated the technical content.

Table of Contents

1 Non-Alphanumeric

@GMT Token: A special token that can be present as part of a file path to indicate a request to see a previous version of the file or directory. The format is "@GMT-YYYY.MM.DD-HH.MM.SS". This 16-bit Unicode string represents a time and date in Coordinated Universal Time (UTC), with YYYY representing the year, MM the month, DD the day, HH the hour, MM the minute, and SS the seconds.

.nsc File: A Windows Media Station file that serves as an announcement of a Media Stream Broadcast Distribution (MSBD) Protocol.

2 0-9

64-bit Network Data Representation (NDR64): A specific instance of an **RPC transfer syntax**. For more information about RPC transfer syntax, see [C706] section 14.

8.3 Name: A file name string restricted in length to 12 characters that includes a base name of up to 8 characters, one character for a period, and up to 3 characters for a file name extension. For more information on 8.3 file names, see [CIFS] section 3.2.

88 Object Class: An object class as specified in [X500]. An 88 object class inherits only from the top. An 88 object class can be instantiated as a new object, like a structural object class, and on an existing object, like an auxiliary object class.

3 A

Abort Request: An action that a participant performs to force a transaction to eventually reach an abort outcome.

Abstract Class: See **Abstract Object Class**.

Abstract Object Class: An object class whose only function is to be the basis of inheritance by other object classes, thereby simplifying their definition.

Abstract Syntax Notation One (ASN.1): A notation to define complex data types to carry a message, without concern for their binary representation, across a network. ASN.1 defines an encoding to specify the data types with a notation that does not necessarily determine the representation of each value. ASN.1 encoding rules are sets of rules used to transform data specified in the ASN.1 language into a standard format that can be decoded on any system that has a decoder based on the same set of rules. ASN.1 and its encoding rules were once part of the same standard. They have since been separated, but it is still common for the terms ASN.1 and **Basic Encoding Rules (BER)** to be used to mean the same thing, though this is not the case. Different encoding rules can be applied to a given ASN.1 definition. The choice of encoding rules used is an option of the protocol designer.

Acceptor: A participant that receives a session or connection request. This role is also known as the "subordinate."

Access Check: A verification to determine whether a specific access type is allowed by checking a **security context** against a **security descriptor**.

Access Control Entry (ACE): An entry in an **access control list (ACL)** that contains a set of user rights and a **security identifier (SID)** that identifies a principal for whom the rights are allowed, denied, or audited.

Access Control List (ACL): A list of **access control entries (ACEs)** that collectively describe the security protections that apply to an object.

Access Mask: A 32-bit value present in an **access control entry (ACE)** that specifies the allowed or denied rights to manipulate an object.

Access Point: A **network access server (NAS)** implementing 802.11.

Access Profile: A set of configuration data for a network access server (NAS) to determine the level of service to provide to an **endpoint**. This configuration data is sent from the **RADIUS server** to the network access server (NAS) as a set of **RADIUS attributes**.

Access Type: An action defined for access such as "read", "write", "full control", control access right "x", and so on. Used in security descriptors.

Account: A user, group, or alias object.

Account Domain: A **domain** (identified by a security identifier (SID)) that is the source of SIDs for which the server is authoritative. The account domain is the same as the primary domain for **domain controllers**.

Account Domain Object (Account Domain): A **domain object** that represents an issuing authority in which user objects can be created. For more information about the concept of an issuing authority, see [MS-SECO] section 2.2.

Account Domain SID: The security identifier (SID) of the account domain object.

Account Group: A **group object** whose members always include the security identifier (SID) of the group in the **authorization context**.

Account Object: An element of a **Local Security Authority (LSA)** policy database that describes the rights and privileges granted by the server to a **security principal**. The security identifier (SID) of the security principal matches that of the account object.

ACE: See **Access Control Entry**.

Acknowledgment (ACK): A signal passed between communicating processes or computers to signify successful receipt of a transmission as part of a communications protocol.

ACL: See **Access Control List**.

Activation: The process of instantiating a DCOM object or class factory.

Active Directory (AD): A general-purpose network directory service.

Active Directory also refers to the Windows implementation of a directory service. Active Directory stores information about a variety of objects in the network. Importantly, user accounts, computer accounts, groups, and all related credential information used by the Windows implementation of Kerberos are stored in Active Directory. Active Directory first became available as part of Windows 2000 and is available as part of Windows 2000 Server products and Windows Server 2003 products, and planned for Windows Server 2008. Active Directory is not present in Windows NT 4.0 or in Windows XP. For more information, see [MS-SECO] section 2.2.2 and [MS-ADTS]

Active Directory Domain: A domain hosted on **Active Directory (AD)**. For more information, see [MS-ADTS].

Active Directory Domain Services (AD DS): See **Active Directory (AD)**.

Active Directory Domain Services is a new term that is replacing the phrase "Active Directory" in the Windows Server 2008 project.

Active Directory Object: A distinct set of named attributes that represent a network resource. **File Replication Service (FRS)** uses **Active Directory** objects to represent servers that participate in replica sets and the topology that File Replication Service (FRS) uses to replicate data.

Active Directory Replication: The process by which the changes that are made to **Active Directory** objects on one **domain controller (DC)** are automatically synchronized with other domain controllers (DCs).

Active Directory Schema: The Microsoft Active Directory schema contains formal definitions of every object class that can be created in an **Active Directory forest**. The schema also contains formal definitions of every attribute that can exist in an **Active Directory** object.

Active Directory Table (ADT): A database of domain information, as specified in [MS-ADTS].

Active Node: A **node** that is currently successfully executing the implementation-specific server-to-server protocols that constitute participation in a **cluster**.

Active Partition: A partition on a **master boot record (MBR)** disk that becomes the system partition at system startup if the BIOS is configured to select that disk for boot. A master boot record (MBR) disk can have exactly one active partition. This attribute is stored within the partition table on the disk.

Active Volume: See **Active Partition**.

AD: See **Active Directory**.

AddRef: The process of calling the second IUnknown method (IUnknown::ADDref()) on an object. For more information, see [MS-DCOM].

Administrative Plug-in GUID: See **Tool Extension GUID**.

Administrative Template: A file associated with a **Group Policy object (GPO)** that combines information on the syntax of registry-based policy settings with human-readable descriptions of the settings, as well as other information.

Administrative Tool: A tool that allows administrators to read and write policy settings to and from a Group Policy object (GPO).

Administrator: A user who has complete and unrestricted access to the computer/domain.

Administrator in Admin Approval Mode or Consent Admin: A user mode in which administrators are prompted for permission before allowing an administrative task to be performed. Also referred to as a "Consent Admin."

Administrators: An alias object with the security identifier (SID) S-1-5-32-544.

Advanced Encryption Standard (AES): A block cipher that supersedes the **Data Encryption Standard (DES)**. AES is used in symmetric-key cryptography and is also known as the Rijndael symmetric encryption algorithm.

Advanced Systems Format (ASF): The file format used by Windows Media.

Advertise: To publish descriptive identifying information in a name service.

Advertised: An installation state of an application on a **client computer**. An advertised application is one that does not have all of the binaries and files necessary for executing the application present on the computer, but does have metadata on the **client** that allows it to present the application to the user as if all the files were present and also allows the client to install all of the missing files at a later time.

Alias Object: See **Resource Group**.

Allocation Unit Size: The size (expressed in bytes) of the units used by the file system to allocate space on a disk for the file system used by the volume. The size, in bytes, must be a power of two and must be a multiple of the size of the sectors on the disk. Typical allocation unit sizes of most file systems range from 512 bytes to 64 KB.

Alternate Stream: See **Named Stream**.

Ambiguous Name Resolution (ANR): A search algorithm that permits a client to search multiple naming-related attributes on objects by way of a single clause of the form "(anr=value)" in an **LDAP** search filter. This permits a client to query for an object when the client possesses some identifying material related to the object but does not know which attribute of the object contains that identifying material.

Ancestor Object: An object **A** is an ancestor of object **O** if there is a directed path from **A** to **O**. In other words, **A** is on the path from **O** to the root of the tree containing **O**.

Anonymous Authentication: An authentication mode in which neither party verifies the identity of the other party

Anonymous Session: A session created for an anonymous user.

Anonymous User: A user who presents no credentials when identifying himself or herself. The process for determining an anonymous user can differ based on the authentication protocol, and the documentation for the relevant authentication protocol should be consulted.

ANSI Character Set: The American National Standards Institute Character Set (also known as Windows-1252), was the standard for the core fonts supplied with U.S. versions of Windows up to, and including, Windows 95, and Windows NT 4.0, prior to the use of Unicode. ANSI is an eight-bit character encoding scheme based on the English alphabet, and is used to extend the ASCII character set. ANSI codes represent a total of 217 text characters in computers, communications equipment, and other devices that work with text. All references to ANSI refer to a single eight-bit ANSI character represented by a 4-digit keyboard code entered by the user (such as ALT+0128 for the Euro currency character), or an array of eight-bit ANSI characters with the high bit of each character set to zero.

Anywhere Access Gateway: A Network Access Server (NAS) that provides remote connectivity to a network.

AP Exchange: See **Authentication Protocol (AP) Exchange**.

Application: A participant that is responsible for beginning, propagating, and completing an atomic transaction. An application communicates with a transaction manager in order to begin and complete transactions. An application communicates with a transaction manager in order to marshal transactions to and from other applications. An application also communicates in application-specific ways with resource manager in order to submit requests for work on resources.

Application Advertise Script: A file that contains a sequence of installation operations and configuration data for installing an application on a client machine. The installer follows the installation operations in the file and configures the metadata of the application to match the state information specified in the script.

Application Configuration File (ACF): A supplemental file that accompanies an **IDL** specification, and is used to specify stub processing rules. For more information, see "The Attribute Configuration Source" in Part 2 of [C706] and [MS-RPCE].

Application Desktop Toolbar: A window (anchored to an edge of the screen) that is similar to the taskbar and that typically contains buttons that give the user quick access to other applications and windows.

Application NC: A specific type of **naming context (NC)**, or an instance of that type, that supports only full replicas (no partial replicas). An **application NC** cannot contain security principal objects. An **application NC** can contain dynamic objects; no other type of naming context (NC) can. A forest can have zero or more application naming contexts (NCs). Application naming contexts (NCs) do not appear in the **global catalog (GC)**. The root of a **domain NC** is an object of class **domainDns**.

Application Protocol: A network protocol that visibly accomplishes the task that the user or other agent wants to perform. This is distinguished from all manner of support protocols: from Ethernet or IP at the bottom, to security and routing protocols. These, while necessary, are not always visible to the user. Application protocols include, for instance, HTTP and SMB.

ASCII: The American Standard Code for Information Interchange (ASCII) is an 8-bit character encoding scheme based on the English alphabet. ASCII codes represent text in computers, communications equipment, and other devices that work with text. In this specification, all references to ASCII refer to a single eight-bit ASCII character or an array of eight-bit ASCII

characters with the high bit of each character set to zero. In this specification, when arrays of ASCII characters are defined, details are included that indicate if the array of ASCII characters are null-terminated.

AS Exchange: See **Authentication Service (AS) Exchange**.

ASN.1: Abstract Syntax Notation One. ASN.1 is used to describe Kerberos datagrams as a sequence of components, sent in messages. ASN.1 is described in the following: [ITUX660] for general procedures; [ITUX680] for syntax specification, and [ITUX690] for the BER, CER, and DER encoding rules.

Note There is a charge to download these documents.

Assigned Application: An application that is to be installed at computer startup or user logon.

Atomic Transaction: A shared activity that provides mechanisms for achieving the ACID properties (atomicity, consistency, isolation, and durability) when state changes occur inside participating resource managers.

Attribute: (1) A characteristic of some object or entity, typically encoded as a name-value pair.

(2) (A specialization of the pervasive concepts definition above.) An identifier for a single or multi-valued data element that is associated with a directory object. An object consists of its attributes and their values. For example, cn (common name), street (street address), and mail (e-mail addresses) can all be attributes of a user object. An attribute's schema, including the syntax of its values, is defined in an attributeSchema object.

Attribute Syntax: Specifies the format and range of permissible values of an attribute. The syntax of an attribute is defined by several attributes on the attributeSchema object. Attribute syntaxes supported by **Active Directory** include Boolean, Enumeration, Integer, LargeInteger, String(UTC-Time), Object(DS-DN), and String(Unicode).

AttributeId: An OID-valued attribute of each attributeSchema object in the schema naming context (NC). In many LDAP directory implementations, the attributeId is the standard internal representation of an attribute. In the directory model used in this specification, the more familiar ldapDisplayName of an attributeSchema object represents an attribute.

AttributeStamp: The type of a stamp attached to an attribute.

Augmented Backus-Naur Form (ABNF): A modified version of Backus-Naur Form (BNF), commonly used by Internet specifications. ABNF notation balances compactness and simplicity with reasonable representational power. ABNF differs from standard BNF in its definitions and uses of naming rules, repetition, alternatives, order-independence, and value ranges. As specified in [RFC4234].

Authenticated IP (AuthIP): An IKE protocol extension. AuthIP is specified in [MS-AIPS].

Authenticated Users: A built-in security group specified in [MS-SECO] whose members include all users that can be authenticated by a computer.

Authentication: (1) The ability of one entity to determine the identity of another entity.

(2) The act of proving an identity to a server while providing key material which binds the identity to subsequent communications.

Authentication Header (AH): An IPsec encapsulation mode that provides authentication and message integrity. For more information, see [RFC4302] section 1.

Authentication Level: A numeric value indicating the level of authentication or message protection that **remote procedure call (RPC)** will apply to a specific message exchange. For more information, see [C706] section 13.1.2.1 and [MS-RPCE].

Authentication Mode: One of several modes in which an authentication exchange may be performed.

Authentication Protocol (AP) Exchange: The Kerberos sub-protocol called the "authentication protocol," sometimes referred to as the "Client/Server Authentication Exchange," in which the client presents a **service ticket** and authenticator to a service to establish an authenticated communication session with the service. The protocol is specified in [RFC4120] section 3.2.

Authentication Server: An entity that provides **authentication services** to **authenticators** so these services don't have to be implemented by the **authenticators**.

Authentication Service (AS): A service that issues **ticket granting tickets (TGTs)**, which are used for authenticating principals within the realm or domain served by the authentication service.

Authentication Service (AS) Exchange: The Kerberos sub-protocol in which the authentication service component of the **key distribution center (KDC)** accepts an initial logon or authentication request from a client and provides the client with a ticket granting ticket (TGT) and necessary cryptographic keys to make use of the ticket. This is specified in [RFC4120] section 3.1. The **AS Exchange** is always initiated by the client, usually in response to the initial logon of a principal such as a user.

Authentication Type: A numeric identifier that uniquely identifies a security provider.

Authenticator: (1) The entity requesting the authentication of a peer.

(2) A protocol message or data structure within a message that carries authentication information.

(3) When used in reference to the Netlogon Protocol, the data stored in the NETLOGON_AUTHENTICATOR structure.

(4) When used in reference to Kerberos, see **Kerberos Authenticator**.

AuthIP: See **Authenticated IP (AuthIP)**.

Authorization: The secure computation of roles and accesses granted to an identity.

Authorization Context: The set of identities for groups and the identity of the user made available to a server for the purposes of determining authorization to a resource.

Authorization Data: An extensible field within a **Kerberos** ticket, used to pass authorization data about the principal on whose behalf the ticket was issued to the application service.

Auxiliary Class: An object class that cannot be instantiated in the directory but which may be associated with an abstract or structural object class to add its attributes to that abstract or structural class.

Auxiliary Object Class: An object class that can be instantiated on, or removed from, an existing object.

AV Pair: Attribute/Value pair. The name of some attribute, along with its value. AV Pairs in **NTLM** have a structure specifying the encoding of the information stored in them.

4 B

Back Link: An attribute whose value refers to a directory object, and whose Attribute-Schema object has an odd value for attribute **linkId**. A back link only exists in response to the existence of a forward link. Forward links can exist with no back links.

Back Link Attribute: A computed attribute whose values include object references (for example, an attribute of syntax Object(DS-DN)). The values are derived from the values of a related attribute, a forward link attribute, on other objects. If **f** is the forward link attribute, one back link value exists on object **o** for each object **r** that contains a value of **o** for attribute **f**. The relationship between the forward and back link attributes is expressed using the **linkId** attribute on the **attributeSchema** objects representing the two attributes. The forward link's **linkId** is an even number, the back link's **linkId** is the forward link's **linkId** plus one. For more information, see [MS-ADTS] section 3.1.1.1.6.

Back Link Value: The value of a **back link attribute**.

Backup Browser Server: A browser server on a subnet that has been chosen by the **local master browser** server on that subnet to be available to share the processing load required to serve browser clients. A **Backup Browser Server** periodically obtains a copy of information concerning available resources on a particular subnet, from the **master browser server** for that subnet.

Backup Domain Controller (BDC): A domain controller (DC) that receives a copy of the domain directory database from the **primary domain controller (PDC)**. There is only one PDC or PDC emulator in a domain and the rest are **backup domain controllers**.

Backup Stream: The components of an Windows NT backup file. It is important not to confuse a backup stream with a named stream. Backup streams are bytes within the main stream of an Windows NT backup file, while a named stream is part of a file that is not an Windows NT backup file that requires a separate open call to access.

Backus-Naur Form: A syntax used to describe context-free grammars, which is a prescribed way to describe languages.

Balloon Tooltip: A tooltip displayed inside a balloon-shaped window. It usually has an icon, a title, and the tooltip text.

Base64: A binary-to-text encoding scheme whereby an arbitrary sequence of bytes is converted to a sequence of printable **ASCII** characters.

Basic Disk: A disk on which each volume can be composed of exclusively one partition.

Basic Encoding Rules (BER): A set of encoding rules for ASN.1 notation. These encoding schemes allow the identification, extraction, and decoding of data structures.

Basic Provider: A **virtual disk service (VDS)** provider that manages basic disks.

Basic Volume: A partition on a **basic disk**.

BDC: See **Backup Domain Controller (BDC)**.

Bidirectional Domain Trust Relationship: Two domains X and Y are said to have a bidirectional trust relationship if there is a **domain trust relationship** from X to Y and also one from Y to X.

Big-Endian: Multiple-byte values that are byte-ordered with the most significant byte stored in the memory location with the lowest address.

Binary Large Object (BLOB): A collection of binary data stored as a single entity in a database.

Binding: The string representation of the protocol sequence, NetworkAddress, and optionally the endpoint. Also referred to as "string binding." For more information, see [C706] section "String Bindings."

BitLocker: BitLocker Drive Encryption. A Microsoft-developed feature appearing in Windows Vista that provides encryption for an entire volume.

Blocking Mode (of a Named Pipe): Determines if input/output (I/O) operations will wait for their entire data to be transferred before returning to the caller. For a write operation, if blocking is enabled, the write request will not complete until the **named pipe** reader has consumed all of the data inserted into the named pipe as part of a write request. If blocking is not enabled, the write will complete as soon as the data has been inserted into the named pipe, regardless of when the data in the named pipe is consumed. For a read operation, if blocking is enabled, the read request will be suspended until data is available to be read. If blocking is not enabled, the read will complete immediately, even if there is no data available to be read.

BNF: See **Backus-Naur Form**.

Boot Configuration File: A file that contains a list of paths to boot partitions. On architectures featuring the **Extensible Firmware Interface (EFI)**, the boot configuration file may be stored on other non-volatile media, such as NVRAM. On all other architectures, it resides in the system partition.

Boot File: A file that contains a list of paths to boot partitions. On some systems, the boot file may be stored on other non-volatile media, such as NVRAM.

Boot Loader: An architecture-specific file that loads the operating system on the boot partition as specified by the boot configuration file.

Boot Loader File: See **Boot Loader**.

Boot Partition: A partition containing the operating system.

Boot Volume: See **Boot Partition**.

Boot.Ini: The name of the **boot loader file** on Windows–based computers.

Boxcar: A set of messages transmitted together by way of an underlying MSDTC Connection Manager: OleTx Transports Protocol session.

Bridgehead Domain Controller: A domain controller (DC) that may replicate updates to or from domain controllers (DCs) in sites other than its own.

Broadcast: A style of resource location where a client makes a request to all parties on the network simultaneously (a one-to-many communication). Also, a mode of resource location that does not use a name service.

Browser: See **Browser Server**.

Browser Client: There are two types of browser clients: workstations and non-browser servers. In the context of browsing, non-browser servers supply information about themselves to browser servers, and workstations query browser servers for information.

Browser Server: An entity that maintains information about other servers and domains.

Bucket Rate: A value in a **TSpec** used to specify an aspect of network traffic behavior, as specified in [RFC2212].

Built-in Administrator: A built-in account for administering the computer/domain.

Built-in Domain: A domain object with the issuing authority security identifier (SID) of S-1-5-32.

Built-in Domain Security Identifier (SID): The security identifier (SID) of the built-in domain object.

Built-in Principal: A default security principal whose security identifier (SID) is identical in every domain.

Bus: Computer hardware to which peripheral devices may be connected. Messages are sent between the CPU and the peripheral devices using the bus. Examples of bus types include SCSI, USB, and 1394.

Bus Type: A type of **bus**. Examples of bus types include SCSI, USB, and 1394.

5 C

CA: See **certificate authority (CA)**.

Canonical name: A syntactic transformation of an Active Directory **distinguished name (DN)** into something resembling a path that still identifies an object within a forest. Distinguished name (DN) "cn=Peter Houston, ou=NTDEV, dc=microsoft, dc=com" translates to the canonical name "microsoft.com/NTDEV/Peter Houston", while the distinguished name (DN) "dc=microsoft, dc=com" translates to the canonical name "microsoft.com/". The name of an object in the DS_CANONICAL_NAME format specified in [MS-DRSR] section 3.3.5.13.

CAPI: See **Cryptographic Application Programming Interface (CAPI) or (CryptoAPI)**.

Causality Identifier (CID): A **GUID** that is passed as part of an **ORPC** call to identify a chain of calls that are causally related.

Certificate: (1) A certificate securely binds a **public key** to the entity that holds the corresponding **private key**. A certificate is commonly used for authentication and secure exchange of information on open networks, such as the Internet, extranets, and intranets. Certificates are digitally signed by the issuing **certificate authority (CA)** and can be issued for a user, a computer, or a service. The most widely accepted format for certificates is defined by the ITU-T X.509 version 3 international standards. A certificate is a collection of attributes and extensions that can be stored persistently. The set of attributes in a certificate may vary depending on the intended usage of the certificate. For more information on attributes and extensions, see [RFC3280] and [X509] sections 7 and 8.

(2) When referring to X.509v3 certificates, that information consists of a public key, a distinguished name (DN) of some entity assumed to have control over the private key corresponding to the public key in the certificate, and some number of other attributes and extensions assumed to relate to the entity thus referenced. Other forms of certificates can bind other pieces of information.

Certificate Authority (CA) (or Certification Authority): (1) A third party that issues public key **certificates**. **Certificates** serve to bind public keys to a user identity. Each user and **certificate authority** may decide whether to trust another user or **CA** for a specific purpose, and whether this trust should be transitive.

(2) A software component that issues digital (**X.509**) **certificates** to identities based on a public/private key pair. For more information, see [RFC2865].

Certificate Chain: A sequence of **certificates**, where each **certificate** in the sequence is signed by the subsequent **certificate**. The last **certificate** in the chain is normally a self-signed **certificate**.

Certificate Issuance: See **Certification**.

Certificate Manager: See **Certificate Authority (CA) (or Certification Authority)**.

Certificate Revocation: The process of invalidating a **certificate**. For more information, see [RFC3280] section 3.3.

Certificate Revocation Lists (CRL): A list of **certificates** that have been revoked by the **certificate authority (CA) (or certification authority)** that issued them (that have not yet expired of their own accord). The list must be cryptographically signed by the **certificate authority (CA)** that issues it. Typically, the **certificates** are identified by serial number. In addition to the serial number for the revoked **certificates**, the **CRL** also contains the

revocation reason for each **certificate** and the time the **certificate** was revoked. As specified in [RFC3280], two types of **CRLs** commonly exist in the industry. Base **CRLs** keep a complete list of revoked **certificates** while delta **CRLs** maintain only those **certificates** that have been revoked since the last issuance of a base **CRL**. For more information, see section 7.3 of [X509], [MSFT-CRL], and section 5 of [RFC3280].

Certificate Services: The Microsoft implementation of a **certificate authority (CA)** that is part of the server operating system. **Certificate Services** include tools to manage issued **certificates**, publish **certificate authority (CA) certificates** and **CRLs**, configure **certificate authorities (CAs)**, import and export **certificates** and keys, and recover archived private keys.

Certificate Store: A database of **certificates**, or **certificates** and the accompanying private key. Used to store a variety of **certificates** with different attributes or constraints.

Certificate Template: A list of attributes that define a blueprint for creating an X.509 **certificate**. It is often referred to in non-Microsoft documentation as a "certificate profile." A **Certificate Template** is used to define the content and purpose of a **digital certificate**, including issuance requirements (certificate policies), implemented X.509 extensions such as application policies, key usage, or extended key usage as specified in [X509], and enrollment permissions. Enrollment permissions define the rules by which a **certificate authority (CA)** will issue or deny certificate requests. In Windows environments, **Certificate Templates** are stored as objects in the Active Directory and used by Microsoft enterprise **CAs**.

Certification: The **certificate** request and issuance process whereby an **end entity (EE)** first makes itself known to a **certificate authority (CA)** (directly, or through a registration authority) through the submission of a certificate enrollment request, prior to that **certificate authority (CA)** issuing a certificate or certificates for that EE.

Challenge: A piece of data used to authenticate a user. Typically a challenge takes the form of a **nonce**.

Challenge-Handshake Authentication Protocol (CHAP): A protocol for user authentication to a remote resource. For more information, see [RFC1994] and [RFC2759].

Challenge/Response Authentication: A common authentication technique whereby a principal is prompted (the challenge) to provide some private information (the response) to facilitate authentication.

Challenge-Response Protocol: A type of authentication protocol where the authentication is carried by sending a challenge from one party to another with the other party providing a response that proves its identity.

Change Journal: The database to which records of file or directory changes are written by the **NTFS** file system. Each volume on a system has its own change journal.

Change Order: A message that contains information about a file or folder that has changed on a replica. The change order is sent to the member's outbound partners. If the outbound partners accept the change, the partners request the associated staging file. After installing the changed file in their individual replica trees, the partners propagate the change order to their outbound partners.

Channel Lifetime: The maximum content length of an IN channel or OUT channel (in bytes).

Channel Recycling: An occurrence of either IN channel recycling or OUT channel recycling.

Checksum: A value that is the summation of a byte stream. By comparing the checksums computed from a data item at two different times, one can quickly assess whether the data items are identical.

Child Object, Children: An object that is not the root of its tree. The children of an object **o** are the set of all objects whose parent is **o**.

Chunks: The pieces of a file defined by the cut points.

Cipher: A cryptographic algorithm used to encrypt and decrypt files and messages.

Ciphersuite: A set of cryptographic algorithms used to encrypt and decrypt files and messages.

Ciphertext: The encrypted form of a message. **Ciphertext** is achieved by encrypting the **plaintext** form of a message, and can be transformed back to plaintext by decrypting it with the proper key. Without that transformation, a **ciphertext** contains no distinguishable information.

Class: User-defined binary data associated with a key.

Class Factory: An object instance or class whose purpose is to create instances of another specific object.

Class Identifier (CLSID): A GUID that identifies an object class.

Class Store Container DN: A distinguished name (DN) of the form "CN=Class Store,<scoped gpo dn>" where <scoped gpo dn> is a Scoped Group Policy object (GPO) distinguished name (DN). The class store container distinguished name (DN) refers to an object of objectClass "classStore" in the Active Directory schema.

Client: (1) A computer on which the **remote procedure call (RPC) client** is executing.

(2) An execution environment that holds object references and issues Object RPC (ORPC) calls.

(3) In **DFS-R**, a replicating machine acts as a client when it receives replicated files from its upstream partner. Use of the terminology **client** stipulates that the machine contact its upstream server, and is responsible for initiating communication related to receiving replicated files. It does not imply anything about the operating system version or the function of the machine.

Client Area: The area of the desktop that is available for a window or notification icon to paint on.

Client Challenge: A 64-bit nonce generated on the client side.

Client Computer: (1) A computer that instigates a connection to a well-known port on a server.

(2) A computer that receives and applies settings from a Group Policy object (GPO), as specified in [MS-GPOL].

Client Context: A context describing an execution environment from which an activation request has originated.

Client Locator: Enables lookup of entries exported to remote procedure call (RPC) name service.

Client/Server Mode: Client/Server Mode consists of one server with many client connections (one-to-many). From the perspective of each client, there is only one connection: the connection to the server.

Client-Side Extension GUID (CSE GUID): A well-known GUID that associates a specific client-side Group Policy plug-in with a set of policy settings that can be stored in a Group Policy object (GPO).

Cluster: A group of computers that are able to dynamically assign resource tasks among nodes in a group.

Cluster Name: The computer name that is associated with a cluster, rather than with a single computer system.

Cluster Size: See **allocation unit size**.

Cluster State: A state that consists of all the non-volatile configuration data and volatile current status data that is maintained by the **cluster** and accessible to active nodes.

CNG: See **Cryptography API: Next Generation (CNG)**.

Coalesced Payload: A special form of payload that consists of multiple traditional payloads combined into a single packet.

Collision-Resistant Hash Function: A hash function having the property that, in practice, differing inputs do not produce the same hash (that is, they do not collide).

Color Profile: A file that contains information about how to convert colors in the color space and the color gamut of a specific device into a device-independent color space. A device-specific color profile is called a "device profile." For more information on using color and device profiles, see [MSDN-UDP].

COM Class: A **CLSID** GUID that is registered on the computer system. The COM Class is a number that uniquely identifies an implementation of a programmable software component.

Commit Request: The action that is performed by a root application to initiate the Two-Phase Commit Protocol for an atomic transaction.

Common Information Model (CIM): An object-oriented information model that provides a conceptual framework for describing management data, as specified in [DMTF-DSP004].

Common Information Model (CIM) Class: A collection of **Common Information Model (CIM)** instances that support the same type, that is, the same CIM properties and **CIM methods**, as specified in [DMTF-DSP004].

Common Information Model (CIM) Instance: Provides values for the **CIM** properties associated with the **CIM instance's** defining **CIM class**. A **CIM instance** does not carry values for any other **CIM** properties or **CIM methods** that are not defined in (or inherited by) its defining **CIM class**. For more information, see [DMTF-DSP004].

Common Information Model (CIM) Method: An operation describing the behavior of a **CIM class** or a **CIM instance**. It is generally an action that can be performed against the manageable entity made of a **CIM class**.

Common Information Model (CIM) Namespace: A logical grouping of a set of **Common Information Model (CIM)** classes designed for the same purpose or sharing a common

management objective within the database used to store all CIM class definitions. This is a term mostly referenced in the WMI implementation.

Common Information Model (CIM) Object: An object that represents a **Common Information Model (CIM)** object. This may be either a **CIM class** or a **CIM instance** of a **CIM class**.

Common Information Model (CIM) Path: A string expression locating a class or an instance of class in the operating system. The **CIM Path** includes the computer name, the namespace, the name of **CIM class** and the unique identifier locating the **CIM class** or **CIM instance**.

Common Information Model (CIM) Property: Assigns values used to characterize instances of a **CIM class**. A **CIM property** can be thought of as a pair of **Get** and **Set** functions that, when applied to an object, return state and set state, respectively. For more information, see [DMTF-DSP004].

Common Information Model (CIM) Qualifier: Used to characterize named elements, as specified in [DMTF-DSP004]. For example, there are **CIM qualifiers** that define the characteristics of a **CIM property** or the key of a **CIM class**.

Common Information Model (CIM) Relative Path: A string expression where elements like the computer and/or the namespace of the **CIM class** and/or **CIM instance** are not used.

Common Name (CN): A string attribute of a **certificate** that is one component of a distinguished name (DN). In Microsoft Enterprise uses, a **CN** must be unique within the forest where it is defined and any forests that share trust with the defining forest. The Web site or e-mail address of the **certificate** owner is often used as a common name. Client applications often refer to a **certificate authority (CA)** by the **CN** of its signing certificate.

Compact Disc File System (CDFS): A file system used for storing files on CD-ROMs.

Component Object Model (COM): An object-oriented programming model that defines how objects interact within a single process or between processes. In **COM**, clients have access to an object through interfaces implemented on the object. For more information, see [MS-DCOM].

Compression Chunk: When compression is used for replication data, the data is divided into smaller units that are suitable for the particular algorithm. The chunk size is specific to the compression algorithm being employed.

Computer: See **Machine**.

Computer Account: See **Machine Account**.

Computer Account Object: An object **o** of class **user** such that **o.userAccountControl** and ADS_UF_WORKSTATION_TRUST_ACCOUNT ≠ 0.

Computer Name: The **DNS** or **NetBIOS** name.

Computer Object: An object of class **computer**. A computer object is a security principal object; the principal is the operating system running on the computer. The shared secret allows the operating system running on the computer to authenticate itself independently of any user running on the system.

Computer Policy Mode: A mode of policy application intended to retrieve settings for the computer account of the client.

Computer-Scoped GPO DN: A scoped Group Policy object (GPO) distinguished name (DN) that begins with "CN=Machine."

Computer-Scoped GPO Path: A scoped **Group Policy object (GPO) Path** that ends in "\Machine."

Configuration Naming Context (Config NC): A naming context (NC) containing configuration information. In Active Directory, a single **Config NC** is shared among all domain controllers (DCs) in the forest.

Connection:

1. Each user that has a session with a server can create multiple share connections, or resource connections, using that user ID. This resource connection is created using a tree connect **server message block (SMB)** and is identified by an SMB TreeID or TID.

2. Firewall rules are specified to apply to connections. Every packet is associated with a connection based on TCP, UDP, or IP endpoint parameters, see [IANAPORT].

3. In DFS-R, a pair of client and server replication partners.

4. In OleTx, an ordered set of logically related messages. The relationship between the messages is defined by the higher-layer protocol, but they are guaranteed to be delivered exactly one time and in order relative to other messages in the connection.

Connection-Oriented NTLM: A particular variant of NTLM designed to be used with connection-oriented remote procedure call (RPC).

Connection-Oriented RPC: A remote procedure call (RPC) protocol dialect built on top of an RPC transport that supports connections. For more information, see [C706] section 12.

Connection Security Rule: A group of settings that specify how and when connections into and out of a client computer should be protected using **Internet Protocol security (IPsec)**.

Connection Type: A specific set of interactions between participants in an OleTx protocol that accomplishes a specific set of state changes. A connection type consists of a bidirectional sequence of messages that are conveyed by using the MSDTC Connection Manager: OleTx Transports Protocol Specification and MSDTC Connection Manager: OleTx Multiplexing Protocol Specification transport protocols, as specified in [MS-CMPO] and [MS-CMP]. A specified transaction typically involves many different connection types during its lifetime.

ConnectionId: A GUID that uniquely identifies a connection.

Connectionless NTLM: A particular variant of NTLM designed to be used with connectionless RPC.

Connectionless RPC: An RPC protocol dialect built on top of an RPC transport that does not support connections. For more information, see [C706] section 12.

Constrained Delegation: A Windows feature used in conjunction with **S4U2proxy**. This feature limits the proxy services for which the application service is allowed to get tickets on behalf of a user.

Constructed Attribute: An attribute whose values are computed from normal attributes (for read) and/or have effects on the values of normal attributes (for write).

Contact Identifier: A **universally unique identifier** that identifies a partner in the MSDTC Connection Manager: OleTx Transports Protocol. These UUIDs are frequently converted to and

from string representations. This string representation MUST follow the format specified in [C706] Appendix A. In addition, the UUIDs MUST be compared, as specified in [C706] Appendix A.

Container: An object in the directory that can serve as the parent for other objects. In the absence of schema constraints, all objects would be containers. The schema allows only objects of specific classes to be containers.

Content Set: See **replicated folder**.

ContentSetId: The GUID assigned to a specific replicated folder within a **replica set**.

Context: A collection of context properties that describe an execution environment.

Context Identifier: A GUID that identifies a **context**.

Context Property: An attribute of an execution environment.

Context Property Identifier: A GUID that identifies a **context property**.

Control Access Right: (1) An extended access right that can be granted or denied on an access control list (ACL).

(2) A variable access type with a specialized access GUID identifying the specific access type.

Control Menu: See **Window Menu**.

Conversation Callback: A remote procedure call (RPC) request/response message exchange initiated by an **RPC Server** and received by an RPC Client. The message exchange is internal to the connectionless RPC engine.

Coordinated Universal Time (UTC): A high-precision atomic time standard that approximately tracks Universal Time (UT). It is the basis for legal, civil time all over the Earth. Time zones around the world are expressed as positive and negative offsets from UTC. In this role, it is also referred to as Zulu time (Z) and Greenwich Mean Time (GMT). In these specifications, all references to UTC refer to the time at UTC–0 (or GMT).

Copychunk Resume Key: A 24-byte value generated by a server message block (SMB) server in response to a request by an SMB **client** that uniquely identifies an open file on the SMB server. A **Copychunk Resume Key** is used by SMB server-side data movement operations between files without requiring the data to be read by the **client** and then written back to the server. This feature is added with the extensions in this document.

Note that this is different from the resume key specified in [CIFS] section 4.3.4 that is returned by the server in response to a TRANS2_FIND_FIRST2 subcommand of an SMB_COM_TRANSACTION2 **client** request.

Core Transaction Manager Facet: The facet that acts as the internal coordinator of each transaction that is inside the transaction manager. The core transaction manager facet communicates with other facets in its transaction manager to ensure that each transaction is processed correctly. To accomplish this, the core transaction manager facet maintains critical transaction state, in both volatile memory and in a durable store, such as in a log file.

Correlation: In an interface definition language (IDL) file, if the runtime properties of one argument dictate what the runtime properties of another argument are allowed to be, the two arguments are said to have **Correlation**, or one argument is said to be correlated to the other.

Crash Dump File: A file that may be created by an operating system when an unrecoverable fault occurs. This file contains the contents of memory at the time of the crash and may be used to debug the problem.

Credential: A previously established authentication data used by a security principal to establish its own identity, such as a password. When used in reference to the Netlogon Protocol, it is the data stored in the NETLOGON_CREDENTIAL structure.

Critical Object: A subset of the objects in the default naming context (NC), identified by the attribute **criticalSystemObject** having the value TRUE. The objects that are marked in this way are essential for the operation of a domain controller (DC) hosting the NC.

Cross Certification: The **certificate** issuance process by which two **certificate authorities (CAs)**, **CA1** and **CA2**, issue specialized certificates so that any **relying party (RP)** that has **CA1** in its trust root but not **CA2** can link from **CA1** to **CA2** and thereby validate **certificates** in the hierarchy under **CA2** and make use of those. For more information on cross-certification, see section 3.5 of [RFC3280]. For an introduction to cross-certificates and cross-certification, see [MSFT-CROSSCERT].

Cross-Certificate: An X.509 digital certificate issued between two existing independent **certificate authorities (CAs)** for the purpose of extending or constraining **PKI** trust hierarchies. A cross-certificate is specified in section 3.3.21 of [X509]. For an introduction to cross-certificates and cross-certification, see [MSFT-CROSSCERT].

crossRef Object: An object residing in the partitions container of the **config NC** that describes the properties of a naming context (NC), such as its DNS name, operational settings, and so on.

Cryptographic Application Programming Interface (CAPI) or (CryptoAPI): Microsoft's Cryptographic application programming interface (API). An API that enables application developers to add authentication, encoding, and encryption to Windows-based applications

Cryptographic Hash Function: A function that maps an input of any length to a short output bit string of fixed length, such that finding an input that maps to a particular bit string of the correct output length, or even finding two inputs that map to the same output bit string, is computationally infeasible. For more information, see [SCHNEIER], chapters 2 and 18.

Cryptographic Service Provider (CSP): A software module that implements cryptographic functions for calling applications.

Cryptographically Generated Address (CGA): IPv6 address for which the interface identifiers (the low-order 64 bits) are generated by computing a **cryptographic hash function** on a public key. The corresponding private key can be used to sign messages sent from this IPv6 address. **CGA** is specified in [RFC3972].

Cryptography API: Next Generation (CNG): The second generation of the **CryptoAPI** and its long-term replacement. **CNG** allows you to replace existing algorithm providers with your own providers and to add new algorithms as they become available. **CNG** also allows the same APIs to be used from user and kernel mode applications.

Curly Braced GUID String: The string representation of a 128-bit Globally Unique Identifier (GUID) using the form {XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}, where X denotes a hexadecimal digit. The string representation between the enclosing braces is the standard representation of a GUID as defined in [RFC4122] section 3. Unlike a **GUIDString**, a **Curly Braced GUID String** includes enclosing braces.

CurrentRefreshTime: The current time, in units of days, measuring the time since the value was initialized.

Cut Points: The locations in a file where **remote differential compression (RDC)** has determined boundary points between blocks, or chunks. The cut points for a particular file depend on the contents of the file and the parameters with which RDC is running.

Cycle: A series of one or more replication responses associated with the same invocation ID, concluding with the return of a new **USN** that defines the high water mark in which to begin the next replication cycle.

Cyclic Redundancy Check (CRC): An algorithm used to produce a checksum (a small, fixed number of bits) against a block of data, such as a packet of network traffic or a block of a computer file. The **CRC** is used to detect errors after transmission or storage. A **CRC** is designed to catch stochastic errors, as opposed to intentional errors. If errors might be introduced by a motivated and intelligent adversary, a **cryptographic hash function** should be used instead.

Cylinder: The set of disk tracks that appear in the same location on each platter of a disk.

6 D

DACL: See **Discretionary Access Control List**.

Data Encryption Standard (DES): A specification for encryption of computer data that uses a 56-bit key developed by IBM and adopted by the U.S. government as a standard in 1976.

Data Recovery Agent (DRA): A logical entity corresponding to an asymmetric key pair, which is configured as part of **Encrypting File System (EFS)** administrative policy by an administrator. Whenever an EFS file is created or modified, it is also automatically configured to give authorized access to all **DRAs** in effect at that time.

Database: (1) For the purposes of the Netlogon RPC, a database is a collection of user accounts, machine accounts, aliases, groups, and policies, managed by a component. The database, or the component managing the database, must expose a mechanism to enable Netlogon to gather changes from and apply changes to the database. Additionally, it must export a database serial number in order to track changes for efficient replication.

(2) In **DFS-R**, the database maintained by Microsoft's implementation of DFS-R maintains the local version chain vector and one record for each resource that is tracked, including **tombstones** for deleted resources, such that deletion of files can be propagated in a timely fashion.

Database Object: A representation of a named set of attribute value pairs that a protocol exposes.

Database Serial Number: A numeric value incremented each time after a database transaction is applied to the database.

Datagram: A style of communication offered by a network transport protocol where each message is contained within a single network packet. In this style, there is no requirement for establishing a session prior to communication, as opposed to a connection-oriented style.

DAV: See **Distributed Authoring and Versioning**.

DC: See **Domain Controller**.

DC in site x: A **domain controller (DC)** such that the site of the **domain controller (DC)** is x.

Decrypting: In cryptography, the process of transforming encrypted information to its original clear text form.

Decryption: In cryptography, the process of transforming encrypted information to its original clear text form.

Default Naming Context Replica (Default NC Replica): The full domain naming context (NC) replica hosted by a **domain controller (DC)**. The default naming context (NC) always contains the **domain controller's** computer object.

Delta-Time: A negative FILETIME. It represents a period of time, expressed in a negative number of 100 nanosecond time slices. For example, a period of 20 minutes is represented as - 720000000000.

De-Serialize: See **Unmarshal**.

Desktop: When a user logs on interactively they are automatically taken to their instance of a user desktop.

Desktop Switch: The act of switching from one user desktop to another, or to the Windows Secure Desktop.

Device: Any peripheral or part of a computer system that can send or receive data.

Device Driver: The software that the system uses to communicate with a device such as a display, printer, mouse, or communications adapter. It is often referred to as just "driver".

DEVMODE: A binary data structure representing the configuration of a print or display device. For more information, see [DEVMODE].

DFS: See **Distributed File System (DFS)**.

DFS-R: The Distributed File System Replication Protocol.

Dictionary Attack: A technique for defeating an authentication mechanism by systematically searching through a large number of possibilities to deduce shared secrets.

Differentiated Services Code Point (DSCP): A value in an IPv4 or IPv6 header used to select a particular set of quality-of-service behavior, as specified in [RFC2474] section 3.

Digest: The fixed length output string from a one-way hash function that takes a variable-length input string and is probabilistically unique for every different input string.

Digital Certificate: See the "digital certificate definition standard" as specified in [X509].

Digital Fingerprint: See **Hash Function**.

Digital Signature: (1) A message authenticator typically derived from a cryptographic operation using an asymmetric algorithm and private key. When a symmetric algorithm is used for this purpose, the authenticator is typically called a **Message Authentication Code (MAC)**. In some usage, the term **Digital Signature** is used to refer to either kind of authenticator, but in this protocol the term digital signature is used only for authenticators created by asymmetric algorithms.

(2) A value generated using a digital signature algorithm, taking as input a private key and an arbitrary-length string, such that a particular verification algorithm is satisfied by the value, the input string, and the public key corresponding to the input private key. For more information, see [SCHNEIER], chapters 2 and 20.

Directed Change Order: A **change order** that is directed to a single outbound partner and produced when the partner is doing a **vvjoin**, such as during initial synchronization.

Directory: (1) In file systems, a folder.

(2) In Active Directory, an organizational unit containing files or other directories within a hierarchical file system.

(3) An information source used to store information about objects such as users, groups, computers, services and other resources, in one or more domains.

(4) A forest.

Directory Object (or Object): An LDAP object, as specified in [RFC2251], that is a specialization of an object as defined in the pervasive concepts section of this glossary. An Active Directory object can be identified by a **dsname**.

Directory Service (DS): A service that stores and organizes information about a computer network's users and network shares, and that allows network administrators to manage users' access to the shares.

DirectPlay: A network communication library included with the Microsoft DirectX application programming interfaces. DirectPlay is a high-level software interface between applications and communication services that makes it easy to connect games over the Internet, a modem link, or a network.

DirectPlay 4: A programming library that implements the IDirectPlay4 programming interface. DirectPlay 4 provides peer-to-peer session-layer services to applications, including session lifetime management, data management, and media abstraction. DirectPlay 4 first shipped with the DirectX 6 multimedia toolkit. Later versions continued to ship up to, and including, DirectX 9. DirectPlay 4 was subsequently deprecated. The DirectPlay 4 DLL continues to ship in current versions of Windows operating systems, but the development library is no longer shipping in Microsoft development tools and SDKs.

DirectPlay 4 Protocol: All DirectPlay 4 messages are sent by using the DirectPlay 4 Protocol, which enables reliable and non-reliable messages, as well as sequenced and non-sequenced messages. The DirectPlay 4 Protocol can be layered on top of multiple lower-level transport protocols via the DirectPlay 4 Service Providers. The details of the DirectPlay 4 Protocol are specified in the DirectPlay 4 Protocol: Reliable Specification ([MC-DPL4R]).

DirectPlay 8: A programming library that implements the IDirectPlay8 programming interface. DirectPlay 8 provides peer-to-peer session-layer services to applications, including session lifetime management, data management, and media abstraction. DirectPlay 8 first shipped with the DirectX 8 software development toolkit. Later versions continued to ship up to, and including, DirectX 9. DirectPlay 8 was subsequently deprecated. The DirectPlay 8 DLL continues to ship in current versions of Windows operating systems, but the development library is no longer shipping in Microsoft development tools and SDKs.

DirectPlay 8 Application: A software process that communicates with one or more software processes over a communications network by using the DirectPlay 8 family of protocols.

DirectPlay 8 Client Application: A DirectPlay 8 application seeking to connect to another DirectPlay 8 application that is hosting a DirectPlay 8 session. When connected, the actual communication between nodes in a DirectPlay 8 session may be client/server or peer to peer. The term "client" in this definition is meant to indicate the role that the DirectPlay 8 client application is taking in the host enumeration process, which is the DirectPlay 8 application that is seeking to find and connect to a host of a DirectPlay 8 session.

DirectPlay 8 Protocol: All DirectPlay8 messages are sent by using the DirectPlay 8 Protocol, which enables reliable and non-reliable messages, as well as sequenced and non-sequenced messages. The DirectPlay 8 Protocol can be layered on top of multiple lower-level transport protocols via the DirectPlay 8 Server Providers. The details of the DirectPlay 8 Protocol are specified in the DirectPlay 8 Protocol: Reliable Specification ([MC-DPL8R]). Note that the DirectPlay 8 Protocol, as described in the DirectPlay 8 Host and Port Enumeration Protocol Specification ([MC-DPLHP]), does not use the DirectPlay 8 Protocol, but interfaces directly with the DirectPlay 8 Service Provider.

DirectPlay 8 Server Application: A DirectPlay 8 application that is hosting a DirectPlay 8 session. When connected, the actual communication between nodes in a DirectPlay 8 session

may be client/server or peer to peer. The term "server" in this definition is meant to indicate the role that the DirectPlay 8 server application is taking in the host enumeration process, which is the DirectPlay 8 application that is currently hosting a DirectPlay 8 session.

DirectPlay 8 Service Provider: The DirectPlay 8 Protocol may be layered on top of multiple different underlying network transport protocols, such as IPv4, IPv6, IPX, and Serial links. A DirectPlay 8 Service Provider is the layer that adapts the DirectPlay 8 Protocol to a particular underlying network transport protocol. The details of the DirectPlay 8 Service Provider are specified in the DirectPlay 8 Protocol: Core and Service Providers Specification ([MC-DPL8CS]).

DirectPlay Name Server (DPNSVR): A forwarding service for enumeration requests that eliminates problems caused by conflicts between port usages for multiple DirectPlay applications.

DirectPlay Protocol: Either the DirectPlay 4 or DirectPlay 8 protocol.

DirectX: Microsoft DirectX is a collection of application programming interfaces for handling tasks related to multimedia, especially game programming and video, on Microsoft platforms.

DirectX Runtime: A set of libraries created for the family of Windows operating systems that provide interfaces to ease the development of video games.

DirectX Software Development Kit (DirectX SDK): A set of libraries (DirectX Runtime) and supporting infrastructure for building applications for those libraries.

DPNID: A 32-bit identification value assigned to a DirectPlay player as part of its participation in a DirectPlay game session.

DirectX Diagnostic (DXDiag): DXDiag.exe is a diagnostic utility included with Windows that is used to test Microsoft DirectX functionality, including DirectPlay traffic.

Discretionary Access Control List (DACL): An access control list (ACL) that is controlled by the owner of an object and that specifies the access particular users or groups can have to the object.

Disk: A persistent storage device that can include physical hard disks, removable disk units, optical drive units, and **LUNs** unmasked to the system.

Disk Adapter: Computer hardware that controls a disk.

Disk Adapter Name: A string of characters returned by a disk adapter. This string of characters is provided by the vendor of the disk adapter and identifies the adapter make or model.

Disk Block: A logical unit consisting of a fixed number of contiguous sectors. Block sizes range from 512 bytes to several kilobytes.

Disk Controller: Computer hardware that controls a disk.

Disk Encapsulation: The process of converting a basic disk to a **dynamic disk**. Encapsulating a disk lays down disk metadata used for managing the disk dynamically.

Disk Extent: A contiguous set of one or more disk sectors. It may be used as a partition or part of a volume, or it may be free, which indicates it is not in use, or it may be unusable for creating partitions or volumes.

Disk Geometry: The disk's three-dimensional address space: a sector address consists of a cylinder number, the track number within the cylinder, and the sector number on that track.

Disk Group: In the context of **dynamic disks**, this term describes a logical grouping of disks.

Disk Group Import: The act of merging a set of disks belonging to one disk group into another set of disks belonging to a second disk group. The result is a single disk group that includes all disks involved in the import.

Disk Group Name: A unique string of characters used to identify a disk group.

Disk Management Remote Protocol: The protocol used to configure disks and volumes in Windows 2000 and Windows XP. For more information, see [MS-DMRP].

Disk Modification Sequence Number: See **Modification Sequence Number**.

Disk Pack: See **Disk Group**.

Disk Platter: A circular disk on which magnetic data is stored. A hard disk drive consists of several platters mounted onto a spindle that spins the disks for a magnetic head to read and write.

Disk Regions: See **Disk Extent**.

Disk Signature: A unique identifier for a disk. For an MBR formatted disk, this identifier is a 4-byte value stored at the end of the master boot record which is located in sector 0 on the disk. For a **GPT** formatted disk, this value is a GUID stored in the GPT disk header at the beginning of the disk.

Disk Type: A disk that is hardware-specific. A disk can only communicate with the CPU using a bus of matching type. Examples of bus types include SCSI, USB, and 1394.

Disk Vendor Name: A string of characters returned by a disk that identifies the disk maker.

Distinguished Encoding Rules (DER): A method for encoding a data object based on BER encoding but with additional constraints. **DER** is used to encode X.509 certificates that need to be digitally signed or to have its signature verified.

Distinguished Name (DN): (1) The distinguished name of an object's parent, preceded by the **RDN** of the object. The root object of a tree has an assigned DN.

(2) In Active Directory, the unique identifier of an object in the Active Directory, as specified in [MS-ADTS] and [RFC2251].

(3) In X.500, the globally unique name string that identifies an entity in an X.500 directory, as specified in [X500]. The **distinguished name (DN)** consists of several components and is used in X.509 certificates to identify the subject and issuer principals, as specified in [X509].

(4) In LDAP, an LDAP distinguished name, as specified in [RFC2251]. The **distinguished name (DN)** of an object is the **DN** of its parent, preceded by the RDN of the object. Example: CN=David Thompson, OU=Users, DC=Microsoft, DC=COM.

Distributed Authoring and Versioning: Servers that allow collaborative editing and managing of files.

Distributed Component Object Model (DCOM): The Microsoft Component Object Model (COM) specification that defines how components communicate over networks, as specified in [MS-DCOM].

Distributed File System (DFS): A file system that logically groups physical shared folders located on different servers by transparently connecting them to one or more hierarchical

namespaces. **DFS** also provides fault-tolerance and load-sharing capabilities. **DFS** refers to the Microsoft DFS available in Windows Server platforms.

Distributed File System (DFS) Client: A computer used to access a **Distributed File System (DFS)** namespace. It also can refer to the **DFS** software on a client that accesses the **DFS** namespace.

Distributed File System (DFS) Client Target Failback: An optional feature that, when enabled, permits a **DFS** client to revert back to a more optimal DFS target at an appropriate time after a **DFS client target failover**. The term "failback" refers to **DFS client target failback**. The DFS Referral Protocol, as specified in [MS-DFSC], describes the mechanisms by which a DFS server provides a list of DFS targets in decreasing order of optimality to the client.

DFS Client Target Failover: When a **DFS referral** response has multiple targets, a **DFS client** attempts to find the first target that is both available and accessible. If the first DFS target in the list is not available or accessible, the **DFS client** determines whether the next target in the list is available and accessible. The client repeats this process until an available and accessible target is found or no more targets are left in the list of targets. **DFS clients** support **DFS client target failover** only for operations involving pathnames. In this specification, the term "failover" refers to **DFS client target failover**.

DFS In-Site Referral Mode: A mode in which **DFS root** or **DFS link** referral requests to a DFS server result in **DFS referral** responses with only those DFS targets in the same **AD DS site** as the **DFS client** requesting the **DFS referral**. When this mode is disabled, there is no restriction on the AD DS site of the targets returned in the referral response. This can be enabled per **DFS namespace**. If there are no DFS targets in the same AD DS site as the client, the **DFS referral** response may be empty.

DFS Link: A component in a **DFS path** that lies below the **DFS root** and maps to one or more **DFS link targets**. Also interchangeably used to refer to a **DFS path** that contains the **DFS link**.

Distributed File System (DFS) Link Target: The mapping destination of a **link**. A link target can be any **UNC** path. For example, a link target could be a share or another **Distributed File System (DFS)** path.

Distributed File System (DFS) Metadata: Information about a **Distributed File System (DFS)** namespace such as namespace name, **DFS** links, **DFS** link targets, and so on, that is maintained by a **DFS** server. For domain-based **DFS**, the metadata is stored in an **Active Directory Domain Services (AD DS)** object corresponding to the **DFS** namespace. For a stand-alone **DFS namespace**, the **DFS root target** stores the **DFS metadata** in an implementation-defined manner, for example, in the registry.

Distributed File System (DFS) Namespace: A virtual view of shares on different servers as provided by **Distributed File System (DFS)**. Each file in the namespace has a logical name and a corresponding address (path). A **DFS namespace** consists of a root and many links and targets. The namespace starts with a root that maps to one or more root targets. Below the root are links that map to their own targets.

Distributed File System (DFS) Namespace, Clustered: A standalone **Distributed File System (DFS)** namespace, which is hosted on a file server cluster.

Distributed File System (DFS) Namespace, Domain-Based: A **DFS namespace** that has configuration information stored in Active Directory. The **DFS namespace** may span over a distributed system that is organized hierarchically into logical domains, each with a **domain**

controller (DC). The path to access the root or a link starts with the host domain name. A domain-based **DFS root** can have multiple root targets, which offers fault tolerance and load sharing at the root level.

Distributed File System (DFS) Namespace, Standalone: A **DFS namespace** that has metadata stored locally on the host server. The path to access the root or a link starts with the host server name. A stand-alone **DFS root** has only one root target. Stand-alone roots are not fault-tolerant; when the root target is unavailable, the entire **DFS namespace** is inaccessible. Stand-alone **DFS roots** can be made fault tolerant by creating them on clustered file servers.

Distributed File System (DFS) Path: Any UNC path that starts with a **DFS root** and is used for accessing a file or directory in a **DFS namespace**.

Distributed File System (DFS) Referral: A **DFS client** issues a **DFS referral** request to a **DFS root target** or a **DC**, depending on the **DFS path** accessed, to resolve a **DFS root** to a set of **DFS root targets**, or a **DFS link** to a set of **DFS link targets**. The **DFS client** uses the referral request process as needed to finally identify the actual **share** on a server that has accessed the leaf component of the **DFS path**. The request for a **DFS referral** is referred to as **DFS referral request**, and the response for such a request is referred to as **DFS referral response**.

Distributed File System (DFS) Referral Request: The request for a **DFS referral**.

Distributed File System (DFS) Referral Response: The response to a **Distributed File System (DFS) Referral Request**.

Distributed File System (DFS) Referral Site Costing: An optional feature, when appropriately enabled for a **DFS namespace**, results in a **DFS referral** response with targets getting grouped into sets based on increasing Active Directory Domain Services (AD DS) site cost from the **DFS client** requesting the referral to the **DFS** target server. When this feature is disabled, referral response consists of at most two target sets: one set consisting of all **DFS** targets in the same Active Directory Domain Services (AD DS) site as the **DFS client** and the other set consisting **DFS** targets that are not in the same Active Directory Domain Services (AD DS) site as the **DFS client**.

Distributed File System (DFS) Root: The starting point of the **DFS namespace**. The root is often used to refer to the namespace as a whole. A **DFS root** maps to one or more root targets, each of which corresponds to a share on a separate server. A **DFS root** has one of the following formats:

\\<ServerName>\<RootName>

\\<DomainName>\<RootName>

where <ServerName> is the name of the root target server hosting the **DFS namespace**; <DomainName> is the name of the domain that hosts the **DFS root**; and is <RootName> is the name of the root of a domain-based **Distributed File System (DFS)**.

<1>

Distributed File System (DFS) Root Scalability Mode: Domain-based **DFS root** targets normally poll the primary domain controller (PDC) to check for any change in the **DFS metadata** of a **DFS namespace**. When the **DFS** server on a **DFS root** target supports this mode, and it is enabled for a **DFS namespace**, the **DFS** server instead polls a **domain controller (DC)** closer to it in terms of Active Directory Domain Services (AD DS) site cost.

Distributed File System (DFS) Root Target: A server that hosts a **DFS root** of a **DFS namespace**. A domain-based DFS namespace can have multiple **DFS root targets**; a stand-alone DFS namespace can have only one **DFS root targets**.

Distributed File System Replication (DFSR): A service that keeps **DFS** folders in sync automatically. **DFSR** is a state-based, multi-master replication system that supports replication scheduling and bandwidth throttling. This is a re-write and new version of File Replication Service (FRS).

Distributed File System (DFS) Remote Procedure Call (RPC): The remote procedure call (RPC) interfaces and methods that make up the Microsoft Distributed File System, Server-To-Server Protocol.

Distributed Link Tracking (DLT): A protocol that enables client applications to track sources that have been sent to remote locations using remote procedure call (RPC) interfaces, and to maintain links to files. It exposes methods that belong to two interfaces, one of which exists on the server (trksvr) and the other on a workstation (trkwks).

DLT: See **Distributed Link Tracking (DLT)**.

DN: See **Distinguished Name**.

Domain Naming Service (DNS) Name: The fully qualified domain name as known by domain naming service, as specified in [RFC1035] and [RFC1123].

Domain: A network of computers that share a user account database. For more information, see [MS-SECO], section 2.2.

<2>

Domain Account: A stored set of attributes representing a principal used to authenticate a user or machine to an Active Directory domain.

Domain Admins: A group with a security identifier (SID) with the **relative ID** value of 512 in the account domain.

Domain Controller (DC): (1) A server within a domain that functions as an authority for purposes of domain membership and is responsible for administration of domain security. A **DC** makes its account database available to other machines in a controlled fashion. There can be multiple **DCs** in a single domain. For more information, see [MS-SECO] section 2.2.2.

(2) In Active Directory, a server on which the Active Directory operating system directory service is installed. It hosts the data store for objects, and interoperates with other **domain controllers (DCs)** to ensure that a local change to an object replicates correctly across all **DCs**. It contains full naming context (NC) replicas of the config NC, **schema NC**, and one of the **domain NCs** in its forest. If it is a **global catalog server**, it contains partial **NC replicas** of the remaining **domain NCs** in its forest. For more information, see [MS-SECO], section 2.2.2.

Domain Controller Account Object: An object in the directory that represents the computer in the role of a **domain controller (DC)**. A DC account is an object **O** in the default naming context (NC) replica of a server such that **O** is of class **computer** and (O.userAccountControl and ADS_UF_SERVER_TRUST_ACCOUNT ¹0).

Domain Controller Locator: A function within a **domain** that provides for location of **domain controller (DC)** and the ability to determine certain properties of **DCs**. For more information, see [MS-ADTS].

Domain Controllers (DCs): A well-known set of machines that host the domain-wide information.

Domain Database: A database where security principal information is stored. This database is Active Directory in the case of a **domain controller (DC)** running on a Windows machine. On a Windows machine that is not a **domain controller (DC)**, this database is a local database, manageable through Security Accounts Manager Remote Protocol, as specified in [MS-SAMR].

Domain Local Group: A security group that is only valid for inclusion within access control lists (ACLs) from its own domain. Its membership may include users, global groups, and universal groups from any domain. It may additionally include, and be a member of, other domain local groups from within its domains.

Domain Master Browser: A server responsible for combining information for an entire domain, across all subnets.

Domain Master Browser Server: A master browser server that is responsible for combining information for an entire domain, across all subnets. A **Domain Master Browser server** is responsible for keeping multiple subnets in synchronization by periodically querying **local master browser servers** for information concerning user accounts, security, and available resources such as printers.

Domain Member (Member Machine): A machine that is joined to a domain by sharing a secret between the machine and the domain.

Domain Naming Context (Domain NC): (1) A partition of the directory that contains information about the domain, and also is replicated with other **domain controllers (DCs)** in the same domain.

(2) A naming context (NC) whose replicas are able to contain security principal objects. No other NC replica can contain security principal objects.

The **distinguished name (DN)** of a **domain NC** takes the form

dc=n1,dc=n2, ... dc=nk

where each ni satisfies the syntactic requirements of a DNS name component. For more information, see [RFC1034]. Such a **distinguished name (DN)** corresponds to the **DNS name**

n1. n2. ... .nk

This is the **DNS name** of the **domain NC**.

domain NCs appear in the GC. A forest has one or more **domain NCs**. The root of a **domain NC** is an object of class **domainDns**.

Domain Name: The name given by an administrator to a collection of networked computers that share a common directory. Part of the domain naming service (DNS) naming structure, domain names consist of a sequence of name labels separated by periods.

Domain Object: A unit of data storage in a **domain** maintained and made available to **domain** members by a **domain controller (DC)**.

Domain Object (Domain): A database object that represents an issuing authority as specified in [MS-SECO], section 2.2. An account is said to be "in" a particular **domain** if the **domain** prefix of its security identifier (SID) is the SID of the particular **domain**.

Domain of Interpretation (DOI): A DOI defines the manner in which a group of protocols uses the **ISAKMP** (as specified in [RFC2408]) framework to negotiate **security associations (SAs)** (for example, identifiers for cryptographic algorithms, interpretation of payload contents, and so on). For example, the IPsec **DOI** (as specified in [RFC2407]) defines the use of the ISAKMP framework for protocols that negotiate **main mode (MM)** and **quick mode (QM)**security associations (SAs). Both **IKE** and AuthIP fall under the IPsec **DOI**.

Domain Prefix: The portion of a security identifier (SID) that refers to the issuing authority SID. For example, the domain prefix of S-1-5-21-397955417-626881126-188441444-1010 is S-1-5-21-397955417-626881126-188441444.

Domain Tree: A set of **domains** that are arranged hierarchically, typically following an accompanying DNS hierarchy, with trusts between parents and children. An example **domain tree** might be **a.example.com**, **b.example.com**, and **example.com**; domain A and domain B each trust **example.com**, but do not trust each other directly. They will have a transitive trust relationship, through **example.com**.

Domain Trust Relationship: A **domain** X said to trust **domain** Y is described as having a **domain trust relationship** to **domain** Y. This means that **domain** X will perform authorization activities using accounts that are authenticated by **domain** Y. By default, no **domain trust relationships** will exist between two **domains**, and a given **domain** will only authorize access using accounts from that **domain**.

Domain User: A user with an account in the **domain's** user account database.

domainDns: A specific object class. The root of a **domain NC** or an application naming context (NC) is an object of class **domainDns**. The **distinguished name (DN)** of such an object takes the form where each ni satisfies the syntactic requirements of a **DNS name** component. For more information, see [RFC1034]. Such a **DN** corresponds to the **DNS name**. This is the **DNS name** of the naming context (NC), and allows replicas of the naming context (NC) to be located using DNS.

Downlevel Trust: A trust in which one of the peers is running Windows NT 4.0.

Downstream Partner: The partner that receives change orders, files, and folders.

Drive: See **Volume**.

Drive Letter: One of the 26 alphabetical characters A-Z, in upper or lowercase that is assigned to a volume. Drive letters serve as a namespace through which data on the volume can be accessed. A volume with a drive letter can be referred to with the drive letter followed by a colon (for example, C:).

Drive Paths: See **Mounted Folder**.

Driver Package: A collection of the files needed to successfully load the driver. This includes the device information (.inf) file, the catalog file, and all of the binaries that are copied by the .inf file.

Driver Store: A secure location on the local hard disk where the entire driver package is copied.

Dsname: (1) A tuple that contains between one and three identifiers for an object. The term **dsname** does not stand for anything. The possible identifiers are the object's GUID (attribute objectGuid), security identifier (SID) (attribute objectSid) and **distinguished name (DN)** (attribute distinguishedName). A **dsname** can appear in a protocol message and as an attribute value (for example, a value of an attribute with syntax Object(DS-DN)).

(2) A **dsname** is a field 3-tuple:

guid: GUID;

sid: security identifier (SID); and

dn: **distinguished name (DN)**.

A **dsname** can appear in a protocol message and as a value of an attribute. In either context, it identifies an object. If all three fields are null, the **dsname** is null.

As a value of an attribute, a **dsname** always contains a non-null GUID and **DN**, and sometimes contains a non-null SID. Such a **dsname** n refers to the unique object o such that o.objectGuid = n.guid. The SID and **DN** are not used for identification in this case.

As a value within a protocol message, a non-null **dsname** n refers to:

1. If n.guid ≠ null, the unique object o such that o.objectGuid = n.guid (failing if no such object); otherwise

2. If n.dn ≠ null, the unique object o such that o.distinguishedName = n.dn (failing if no such object); otherwise

3. The unique object o such that o.objectSid = n.sid.

Note that the SID is used only if no other part of the dsname is specified.

If o is an object, the function dsname(o) equals [o.objectGuid, o.objectSid, o.distinguishedName].

Dynamic Disk: A disk on which volumes may be composed of more than one partition on disks of the same pack. This is as opposed to basic disks where a partition and a volume are equivalent.

Dynamic Endpoint: A network-specific server address that is requested and assigned at run time. For more information, see [C706].

Dynamic Host Configuration Protocol (DHCP) Client: An Internet host using Dynamic Host Configuration Protocol (DHCP) to obtain configuration parameters such as network addresses.

Dynamic Host Configuration Protocol (DHCP) Scope: The full consecutive range of possible IP addresses for a network. Scopes typically define a single physical subnet on a network to which DHCP services are offered. Scopes also provide the primary way for the server to manage distribution and assignment of IP addresses and any related configuration parameters to clients on the network.

Dynamic Host Configuration Protocol (DHCP) Server: A computer running a DHCP service that offers dynamic configuration of IP addresses and related information to DHCP-enabled clients.

Dynamic Object: An object with a time-to-die (attribute msDS-Entry-Time-To-Die). The directory service garbage-collects a **dynamic object** immediately after its time-to-die has passed. The constructed attribute entryTTL gives a **dynamic object's** current time-to-live, that is, the difference between the current time and msDS-Entry-Time-To-Die. For more information, see [RFC2589].

Dynamic Provider: A Virtual Disk Service (VDS) provider that manages dynamic disks.

Dynamic Volume: A volume on a dynamic disk.

Dynamic Volume Sub-disk: See **Disk Extent**.

7 E

EAP: See **Extensible Authentication Protocol (EAP)**.

EAP Identity: The identity of the **EAP** peer as specified in [RFC3748].

EAP Method: An authentication mechanism that integrates with **EAP**; for example, EAP-TLS, Protected EAP v0 (PEAPv0), EAP-MSCHAPv2, and so on.

EAP Server: The backend authentication server; typically a RADIUS (as specified in [RFC2865]) server.

Echo Request: A message sent to an inbound proxy or outbound proxy in order to elicit a response.

Echo Response: A message sent by an inbound proxy or outbound proxy in response to an echo request.

Empty CIM Object: A data structure confirming to the WMI serialization model having no properties, no method, no derivation.

Encapsulate: See **Disk Encapsulation**.

Encapsulating Security Payload (ESP): An Internet Protocol security (IPsec) encapsulation mode that provides authentication, data confidentiality, and message integrity. For more information, see [RFC4303] section 1.

Encoding: The binary layout used to represent a **CIM object**, whether a CIM class or CIM instance definition. The encoding is what is actually transferred by the protocol.

Encrypting File System (EFS): The name for the **encryption** capability of the NTFS file system. When a file is encrypted using **EFS**, a symmetric key known as the **file encryption key (FEK)** is generated and the contents of the file are encrypted with the FEK. Then, for each user or data recovery agent (DRA) authorized to access the file, a copy of the FEK is encrypted with that user's or DRA's public key and is stored in the file's metadata. For more information about **EFS**, see [MSFT-EFS].

Encryption: In cryptography, the process of obscuring information to make it unreadable without special knowledge.

Encryption Key: One of the input parameters to an encryption algorithm. Generally speaking, an encryption algorithm takes as input a clear-text message and a key, and results in a cipher-text message. The corresponding decryption algorithm takes a cipher-text message, and the key, and results in the original clear-text message.

End Entity (EE): The keyholder (person or computer) to whose key or name a particular certificate refers.

Endpoint: (1) A client on the network that is requesting access to a network access server (NAS). (2) A network-specific address of an RPC server process for remote procedure calls. The actual name and type of the endpoint depends on the RPC protocol sequence being used. For example, for RPC over TCP (RPC Protocol Sequence ncacn_ip_tcp), an endpoint might be TCP port 1025. For RPC over Server Message Block (SMB) (RPC Protocol Sequence ncacn_np), an endpoint might be the name of a named pipe. For more information, see [C706].

Endpoint Mapper: A service on an RPC Server that maintains a database of **dynamic endpoints** and allows clients to map an interface/object UUID pair to a local dynamic endpoint. For more information, see [C706].

Enforcement Client: An enforcement client, as specified in [MSDN-NAP], uses the health state of a computer to request a certain level of access to a network.

Enhanced Key Usage (EKU): An extension that is a collection of **object identifiers (OIDs)** that indicate the applications that use the key.

Enhanced Metafile Format (EMF): A file format that supports the device-independent definitions of images.

Enhanced Metafile Format Plus Extensions (EMF+): A file format that supports the device-independent definitions of images.

Enhanced Metafile Format Spool Format (EMFSPOOL): A format that specifies a structure of **Enhanced Metafile Format (EMF)** records used for defining application and device-independent printer **spool files**.

Enroll/Enrollment: See Certification.

Enrollment Permissions: A list of administrator-defined rights or access control lists (ACLs) that define the capability of a given client (user, machine or device). Enrollment permissions may define a client capability to read a certificate template, write a certificate template, enroll for a certificate based on a specified certificate template, auto-enroll for a certificate based on a specified certificate template or change permissions on a certificate template. Enrollment permissions are stored on a certificate template and are be enforced by the certificate authority (CA). For more information, see [MSFT-TEMPLATES].

Enterprise Certificate Authority: A certificate authority (CA) that is a member of a domain, and uses the directory services of that domain to store policy, authentication, and other information related to the operation of the certificate authority (CA).

Environment Variables: A set of string name/value pairs used to abstract host-specific parameters, such as the location of operating system or installed binaries.

Envoy Context: A context that is marshaled and returned to a client as a result of obtaining an object reference.

Error Code: An integer indicating success or failure. In Microsoft implementations, this is defined as a Windows Error Code. A zero value indicates success; a non-zero value indicates failure.

Error Correction Object: A block of data that contains the error correction data specified by the FEC algorithm. When included, it is located between the ASF Data Packet Error Correction Data and the MSBPACKETHEADER.

Error Record: A structured description of an occurrence of an error.

Error Sequence: An ordered sequence of error records, such that error record N+1 is the immediate error cause for error record N.

Exchange: A pair of messages, consisting of a request and a response.

Exchange Certificate: A certificate that can be used for encryption purposes. This certificate can be used by clients to encrypt their private keys as part of their certificate request. In

Windows environments, an enterprise certificate authority (CA) creates an **exchange certificate** periodically (by default, weekly), and returns the **exchange certificate** upon request of a client. For more information, see [MSFT-ARCHIVE].

Exchange Type: A specification of the format and number of messages in each phase of the IKE protocol.

Expired Channel: An IN channel or OUT channel whose maximum content length has been reached or exceeded, and can no longer accept any **protocol data unit (PDU)** awaiting transmission.

Expunge: To permanently remove an object from a naming context (NC) replica, without converting it to a tombstone.

Extended Key Usage (EKU): An X.509 certificate extension that indicates one or more purposes for which the certificate may be used.

Extended Mode (EM): An optional phase of AuthIP negotiation during which the peers perform a second round of authentication. This phase does not exist in the IKE protocol.

Extended Partition: A construct used to partition a disk into logical units. A disk may have up to four primary partitions or up to three primary partitions and one extended partition. The extended partition may be further subdivided into multiple logical drives.

Extensible Authentication Protocol (EAP): A framework for authentication used to provide a pluggable model for adding authentication protocols for use in network access authentication, as specified in [RFC3748].

Extensible Firmware Interface (EFI): A system developed by Intel designed to replace the BIOS. It is responsible for bootstrapping the operating system on GUID partitioning table disks.

External Trust: A type of trust that refers to a node trusting a domain that is outside the forest in which the node participates.

Extrinsic Event: An event generated by a component outside the implementation.

8 F

Facet: In **OleTx**, a subsystem in a **transaction manager** that maintains its own per-transaction state and responds to intra-transaction manager events from other **facets**. A **facet** can also be responsible for communicating with other participants of a **transaction**.

Failback: A failback operation. The process of returning production to its original location after a primary system failure or scheduled maintenance period.

Failover: A backup operation that automatically switches to a standby database, server, or network if the primary system fails or is temporarily shut down for servicing. **Failover** is an important fault tolerance function of mission-critical systems that rely on constant accessibility.

To the user, **failover** automatically and transparently redirects requests from the failed or down system to the backup system that mimics the operations of the primary system.

A **failover** operation is always followed by a **failback** operation, which is the process of returning production to its original location.

Failover Cluster: A set of independent computers that work together to increase the availability of services and applications. In [MS-CMRP], the term **cluster** is used as shorthand to mean the same thing as **failover cluster**.

Fast Reconnect: A shortcut negotiation that capitalizes on information exchanged in the initial authentication to expedite the reestablishment of a session.

FAT: See **File Allocation Table (FAT)**.

FAT File System: A file system used by MS-DOS and other Windows operating systems to organize and manage files. The **file allocation table (FAT)** is a data structure that the operating system creates when you format a volume by using FAT or FAT32 file systems. The operating system stores information about each file in the **file allocation table (FAT)** so that it can retrieve the file later.

FAT32 File System: A derivative of the **file allocation table (FAT)** file system. FAT32 supports smaller cluster sizes and larger volumes than FAT, which results in more efficient space allocation on FAT32 volumes. FAT32 uses 32-bit addressing.

Fault-Tolerant: The ability of computer hardware or software to ensure data integrity when hardware failures occur. **Fault-tolerant** features appear in many server operating systems and include mirrored volumes and RAID-5 volumes. A **fault-tolerant** volume maintains more than one copy of the volume's data. In the event of disk failure, an alternate copy of the data is still available.

Fault-Tolerant Mirror Set: A volume configuration such that more than one copy of the **volume data** is maintained. Each copy of the data is placed on separate sets of disks. If a disk in one disk set fails, the volume's data is still available on the second set of disks.

Fence: An auxiliary time stamp included in an update.

Fiber Channel Bus: A bus technology that uses optical fiber for communication.

Fid: An SMB file identifier (Fid) is a 16-bit value that the SMB server uses to represent an opened file, Named Pipe, printer, or device. A Fid is returned by an SMB server in response to a client request to open or create a file, Named Pipe, printer, or device. The SMB server guarantees the Fid value returned is unique for a given SMB Connection until the SMB

Connection is closed, at which time the Fid value may be reused. The Fid is used by the SMB client in subsequent SMB commands to identify the opened file, Named Pipe, printer, or device.

File: An entity of data in the file system that a user can access and manage. A file must have a unique name in its directory. It consists of one or more streams of bytes that hold a set of related data, plus a set of attributes (also called properties) that describe the file or the data within the file. The creation time of a file is an example of a file attribute.

File Allocation Table (FAT): A data structure that the operating system creates when you format a volume by using FAT or FAT32 file systems. The operating system stores information about each file in the **file allocation table** so that it can retrieve the file later.

File Allocation Units: Units of a specific size that are used by the file system to allocate space on a disk for the file system used by the volume.

File Attribute: A 32-bit bitmask containing information on a file's properties. For instance, 0x00000001 is used for the read-only attribute.

FileData: What a user traditionally thinks of as a file in typical operating systems, such as a word processor document.

File/Directory Attributes: The attributes of a file or a directory, as specified in [MS-FSCC].

File Encryption Key (FEK): The symmetric key that is used to encrypt the data in an Encrypting File System (EFS)-protected file. The **FEK** is further encrypted and stored in the file metadata such that only authorized users can access it.

File Event Time: The time at which a change to a file or folder is made. This may not be the same as the file create or last-write time. Restoring a file from a backup tape preserves the file create and last-write times, but the file event time is the time when the actual file restoration was performed.

File Extension: The sequence of characters in a file's name between the end of the file's name and the last "." character. Vendors of applications choose such sequences for the applications to uniquely identify files that were created by those applications. This allows file management software to determine which application should be used to open a file.

File GUID: An identifying property of a file or folder in a replica tree. **File Replication Service (FRS)** creates and manages file globally unique identifiers (GUIDs), which, along with the replication version number and event time, are stored in the IDTable. Each file and folder stores its file GUID as part of its attributes; therefore, corresponding files and folders across all replica set members have the same file GUID.

FileId: (1) A 64-bit value used to represent a file. The value of a **FileId** is unique on a single volume of a local file system or a remote file server. A **FileId** is not guaranteed to be unique across volumes, but the file system on the server must guarantee it is unique within a given volume if **FileIds** are supported. **FileIds** are not supported by all local file systems. On Windows, NTFS supports **FileIds**, but the **file allocation table (FAT)** file system does not support them.

(2) The FileLocation of a file at the time it was originally created. A file's **FileId** never changes.

FileInformation: Information that is maintained about a file, such as its **FileId**.

FileLinkInformation: Information about the file necessary to identify and locate a file, including the file's last known Universal Naming Convention (UNC) name, the **MachineID** of the computer on which the file was last known to be located, the last known **FileLocation** of the file, and the file's permanent **FileID**.

FileLocation: A **VolumeID** with an appended **ObjectID**, which together represent the location of a file at some point in time, though the file may no longer be there.

File Property: See **File Attribute**.

File Replication Service (FRS): One of the services offered by a domain controller, which is advertised through the Domain Controller Location protocol. The service being offered to clients is a replicated data storage volume associated with the default naming context (NC).

File Stream: See **Main Stream** and Named Stream.

File System: A system that enables applications to store and retrieve files on storage devices. Files are placed in a hierarchical structure. The file system specifies naming conventions for files and the format for specifying the path to a file in the tree structure. Each file system consists of one or more drivers and dynamic-link libraries that define the data formats and features of the file system. File systems can exist on the following storage devices: diskettes, hard disks, jukeboxes, removable optical disks, and tape backup units.

File System Control (FSCTL): A command issued to a file system to alter or query the behavior of the file system and/or set or query metadata associated with a particular file or the file system itself.

File System Extension: The act of extending the file system on a volume to include more disk sectors. If the size of the volume is larger than the size of the file system for that volume, the file system may be extended to manage more of the volume's disk extensions.

File System Flags: A set of values used by a file system to configure and report file system features and operations.

File System Label: A non-unique string of characters that the file system assigns to the volume, as specified by the user when formatting the volume.

FileTable: Maps a **FileLocation** or **FileID** to a current **FileLocation**.

FILETIME: A 64-bit value representing a time, as specified in [MS-RPCE], Appendix A.

File Version Number: A property of a file and folder in a **replica tree** that is incremented each time the file or folder is updated. The file version number is used to resolve concurrent updates originating from more than one member of the replica set. The version number is only incremented by the member that originated the file update. Other members that propagate the update do not change the version number.

Filter: (1) A setting that excludes subfolders (and their contents) or files from replication.

(2) In the context of the LDAP protocol, the **filter** is one of the parameters in a search request. The **filter** specifies matching constraints for the candidate objects.

(3) A configuration on a network access server (NAS) that specifies the types of traffic that are acceptable for IP local host traffic. **Filters** can block or allow traffic by IP address, IP protocol, TCP port, or UDP port.

Filter Max: The chunking algorithm used in RDC to split files into chunks. With Filter Max, chunk boundaries are determined by local maxima for a fixed horizon size h. The local maxima may be determined by comparing hash values summarizing a limited window of bytes around each file position.

Finite State Machine: A computer, or operating system, in which a set of inputs determines not only the set of outputs but also the internal state of a computer, so that processing is optimized.

Firewall Rule: A group of settings that specify which connections are allowed in to and out of a client computer.

Fixup: A location in a program image depending on an absolute address. Because Win32 programs must be able to run at any address, the linker writes a fixup table to the PE file containing a list of all such locations in the program. Windows will process the fixup table when the program is loaded. RTTarget-32 performs this function in the locate process.

Fix-Up Servers: See **Remediation Server**.

Flags: A set of values used to configure or report options or settings.

Flexible Single Master Operation (FSMO): See **FSMO Role**, **FSMO Role Owner**, and **FSMO Object**.

Flow: A TCP session or UDP pseudo-session, identified by a 5-tuple (source and destination IP and ports, and protocol). By extension, a request/response ICMP exchange (for example, ICMP echo) is also a flow.

Folder: A file system construct. File systems organize a volume's data by providing a hierarchy of objects known as folders or directories, which contain files.

Folder Redirection: The ability to change the location of certain pre- determined folders in a file system from their default location to another location on the same machine or to a network storage location.

Foreign: A dynamic disk group that is not part of a machine's primary disk group. The term **foreign** denotes foreign to this machine. **Foreign** disk and **foreign** disk groups are not online and this means that these disks may not be configured and no data input/output (I/O) to the disks or the volumes on the disks is permitted.

Forest: (1) One or more domains that share a common schema and trust each other transitively. An organization can have multiple **forests**. A **forest** is the security and administrative boundary for all objects that reside within the **forest**. In contrast, a domain is the administrative boundary for managing objects, such as users, groups, and computers. In addition, each domain has individual security policies and trust relationships with other domains.

(2) In Active Directory, a **forest** is a set of naming contexts (NCs) consisting of one schema naming context (NC), one Config naming context (NC), and one or more domain naming contexts (NCs). Because a set of naming contexts (NCs) can be arranged into a tree structure, a **forest** is also a set of one or several trees of naming contexts (NCs).

Forest Functional Level: A specification of functionality available in a **forest**. Must be consistent with the Windows versions of the domain controllers (DCs) in the forest. Possible values in Windows Server 2003 are Win2K, Win2K interim, and Win2K3.

Forest Trust Information: Information about namespaces, domain names, and security identifiers (SIDs) owned by a trusted **forest**.

Format: When a volume is formatted, metadata is written to the disk, which is used by the file system to organize the data on the disk. A volume is **formatted** with a specific file system.

Forward Link Attribute: An attribute whose values include object references (for example, an attribute of syntax Object(DS-DN)). The forward link values can be used to compute the values of a related attribute, a back link attribute, on other objects. If an object **o** refers to object **r** in forward link attribute **f**, and there exists a back link attribute **b** corresponding to **f**, then a back link value referring to **o** exists in attribute **b** on object **r**. The relationship between the forward and back link attributes is expressed using the **linkId** attribute on the **attributeSchema** objects representing the two attributes. The forward link's **linkId** is an even number, the back link's **linkId** is the forward link's **linkId** plus one. A forward link attribute can exist with no corresponding back link attribute, but not vice-versa. For more information, see [MS-ADTS].

Forward Link Value: The value of a forward link attribute.

Forwardable: A flag, as specified in [RFC4120] section 2.6, used in a **S4U2self** KRB_TGS_REQ message to request the resulting service ticket be marked as forwardable, allowing it to be used in a subsequent S4U2proxy KRB_TGS_REQ message.

Free Space: Space on a disk not in use by any volumes, primary partitions, or logical drives.

FrontPage: The FrontPage Server Extensions. These extensions are used by some clients to manage resources/documents on Microsoft's Web servers. These extensions are a series of CGI and POSTs for server side processing.

FRS: See **File Replication Service (FRS)**.

FSCTL: See **File System Control**.

FSMO Object: The object in the directory that represents a specific **FSMO Role**. This object is a member of the **FSMO Role** and contains the **fSMORoleOwner** attribute.

FSMO Role: A set of objects that may be updated in only one naming context (NC) replica at any given time. For more information, see [MS-ADTS].

FSMO Role Abandon: A request to a domain controller (DC) "d". The effect is for d to request the current holder of a specified **FSMO Role** to transfer the role to d. Abandon is typically initiated by the current role holder in anticipation of being unable to host the role, for example, because the domain controller (DC) is being decommissioned. Saying "DC x abandoned the y role" means that x, the current holder of role y, picked another domain controller (DC) "d" and made an **FSMO Role** role y abandon request to d.

FSMO Role Owner: The domain controller (DC) holding the naming context (NC) replica in which the objects of an **FSMO Role** can be updated.

FSMO Role Transfer: A request to a domain controller (DC) "d". If d is the current holder of the specified **FSMO Role**, the effect is to transfer that role to the client; if d is not the current holder of the role, the effect is to update the client's role objects from d's replica, so the client can try the request again on another domain controller (DC).

Full Database Synchronization: A mechanism for synchronizing an entire database record set on a particular replication partner.

Full Format: A format in which all data sectors for the volume are initialized at the time the file system metadata is created.

Full NC Replica: A naming context (NC) replica that contains all attributes of the objects it contains. A full replica accepts originating updates.

Full Token: A **token** that consists of all administrator rights and privileges.

Fully Qualified Domain Name (FQDN): (1) In DNS, an unambiguous domain name that specifies the node's position in the domain naming service (DNS) tree hierarchy absolutely.

(2) In Active Directory, the full name of an object in Active Directory. This name is used by clients to refer to specific objects in Active Directory.

9 G

Game: An application that uses a DirectPlay Protocol to communicate between computers.

Garbage Collection: The process of identifying logically deleted objects (also known as tombstones) and link values that have passed their tombstone lifetime and then permanently removing these objects from a naming context (NC) replica. **Garbage collection** does not generate replication traffic.

GC: See **Global Catalog (GC)**.

GC Server: See **Global Catalog Server**.

Generic Security Services (GSS): An Internet standard (as specified in [RFC2743]) for providing security services to applications. It consists of an API (GSS-API) set, as well as standards that describe the structure of the security data.

Ghosting: Custom client behavior where file contents are downloaded lazily in response to applications accessing files.

Global Catalog (GC): A unified partial view of multiple naming contexts (NCs) in a distributed partitioned directory. Active Directory's **global catalog (GC)** is implemented by **GC** servers.

Global Catalog Server: A domain controller (DC) containing a naming context (NC) replica (one full, the rest partial) for each domain naming context in the forest.

Global Group: Also called domain global group. An Active Directory group that can appear in Access Control Lists (ACLs) anywhere in the forest, and can contain other global groups and users from its own domain. Universal groups can contain domain global groups.

Global Version Sequence Numbers (GVSN): DFS-R associates a pair: (machine identifier, version sequence number) to identify a resource and its version globally.

Globally Unique Identifier (GUID): A 128-bit value with a low statistical likelihood of being duplicated, used in cross-process communication to identify entities such as client and server interfaces and remote procedure call (RPC) objects. For more information, see [C706]. See also Universally Unique Identifier.

governsId: An OID-valued attribute of each classSchema object in the schema naming context (NC). In many LDAP directory implementations, the governsId is the standard internal representation of an object class name. In the directory model used in this specification, the more familiar lDAPDisplayName of the classSchema object names an object class.

Group: A set of objects.

Group Object: (1) A database object that represents a collection of user and group objects and has a security identifier (SID) value.

(2) In Active Directory, a group object has object class group. A group has a forward link attribute member; the values of this attribute either represent elements of the group (for example, objects of class **user** or **computer**) or represent subsets of the group (objects of class **group**). The back link attribute **memberOf** enables navigation from group members to the groups containing them. Some groups represent groups of security principals and some do not (and are, for instance, used to represent e-mail distribution lists).

Group Policy: A mechanism that allows one to specify managed configurations for users and computers in an Active Directory service environment.

Group Policy Extension: A protocol mechanism that extends the basic capability of the Group Policy protocol as specified in [MS-GPOL].

Group Policy Object (GPO): A collection of administrator-defined specifications of the policy settings that can be applied to groups of computers in a domain. Each **GPO** includes two elements: an object which resides in the Active Directory for the domain, and a corresponding file system subdirectory which resides on the **sysvol**DFS share of the **Group Policy server** for the domain.

Group Policy Object (GPO) Container Version: A **Group Policy object (GPO)** version stored in the Active Directory portion of the **GPO**.

Group Policy Object (GPO) Distinguished Name (DN): An LDAP distinguished name (DN) for an Active Directory object of object class **groupPolicyContainer**. All such object paths will be paths of the form "LDAP://<gpo guid>,CN=policies,CN=system,<rootdse>" where <rootdse> is the root DN path of the Active Directory domain and <gpo guid> is a **Group Policy object (GPO) GUID**.

Group Policy Object (GPO) File System Version: A **Group Policy object (GPO)** version stored in the file system portion of the **GPO**.

Group Policy Object (GPO) GUID: A curly braced GUID string that uniquely identifies a **Group Policy object (GPO)**.

Group Policy Object (GPO) Path: A domain-based Distributed File System (DFS) path for a directory on the server that is accessible through the DFS/SMB protocols. This path will always be a UNC path of the form: "\\<dns domain name>\sysvol\<dns domain name>\policies\<gpo guid>", where <dns domain name> is the DNS domain name of the domain and <gpo guid> is a **Group Policy object (GPO) GUID**.

Group Policy Object (GPO) Version: A version number that combines the user and machine **Group Policy object (GPO)** versions as one 32-bit quantity. The upper 16 bits of the integer are the user **GPO** version and the bottom 16 bits of the integer are the machine **GPO** version.

Group Policy Server: A server holding a database of **Group Policy objects (GPOs)** that can be retrieved by other machines.

Guest Account: A security account available to users who do not have an account on the computer.

GUID: See **Globally Unique Identifier (GUID)**.

GUID Partitioning Table (GPT): A disk-partitioning scheme that is used by the Extensible Firmware Interface (EFI). **GPT** offers more advantages than master boot record (MBR) partitioning because it allows up to 128 partitions per disk, provides support for volumes up to 18 exabytes in size, allows primary and backup partition tables for redundancy, and supports unique disk and partition IDs through the use of **Globally Unique Identifiers (GUIDs)**. Disks with **GPT** schemes are referred to as GPT disks.

GUID Partitioning Table (GPT) Disk: A disk with **GUID Partitioning Table (GPT)** schemes.

GUID-Based DNS Name: The DNS name of a domain controller (DC), constructed by concatenating the dashed string representation of the objectGUID of the DC's nTDSDSA object, the string "._msdcs.", and the syntactic transformation of the root domain's distinguished name (DN) to a DNS name.

GUIDString: A **Globally Unique Identifier (GUID)** in the form of a null-terminated ASCII or Unicode string, consisting of one group of 8 hexadecimal digits, followed by three groups of 4 hexadecimal digits each, followed by one group of 12 hexadecimal digits. For example, "6B29FC40-CA47-1067-B31D-00DD010662DA". Unlike a Curly Braced GUID String, a **GUIDString** is not enclosed in braces.

10 H

H3 Hash: A hash calculated using the H3 **hash function**.

Handle: Any token that can be used to identify and access an object such as a device, file, or a window.

Handshake: An initial negotiation between peer and authenticator that establishes the parameters of their transactions.

Hard Disk: A peripheral device that provides persistent data storage and does not have removable media.

Hard Disk Drive: A **disk drive** that controls the positioning, reading, and writing of the **hard disk**.

Hard Disk Physical Name: An implementation-specific path that can be used to refer to a specific hard disk on a machine.

Hash-Based Message Authentication Code (HMAC): A mechanism for message authentication using cryptographic hash functions. **HMAC** can be used with any iterative cryptographic hash function (for example, MD5 and SHA-1) in combination with a secret shared key. The cryptographic strength of **HMAC** depends on the properties of the underlying **hash function**.

Hash Function: A function that takes an arbitrary amount of data and produces a fixed length result ("hash") that depends only on the input data. A hash function is sometimes called a **message digest** or a **digital fingerprint**.

Hash Window: The length, in bytes, of the domain of the **rolling hash function**. That is, the parameter *n* in the definition of rolling hash function.

Hashes and Checksums: The collision-resistant substrate of a sequence of bytes. Well-known hash algorithms for computing hashes include MD4, MD5, and SHA-1.

Health Certificate: (1) A digital certificate that is used to authenticate the health status of a **NAP** Client.

(2) An X.509 certificate used to certify the health state of a machine as determined by the policies administered for a network.

Health Certificate Enrollment Agent (HCEA): The client-side component in Health Certificate Enrollment Protocol. The **HCEA** is responsible for receiving health certificates from a **health registration authority (HRA)**. This term can also be used to refer to the client machine in Health Certificate Enrollment Protocol.

Health ID: An identifier of a component or service that supplies host status information in a **statement of health (SoH)** message or that performs evaluation of host status information in a **Statement of Health Response (SoHR)** message.

Health Messages: The set of messages exchanged between peers or clients and servers. These messages are of the types Statement of Health (SoH), and Statement of Health Response (SoHR).

Health Policy Server: An entity in a network that has network polices administered on it and that is capable of validating a Statement of Health (SoH) against the specified polices.

Health Registration Authority (HRA): The server-side component in the Health Certificate Enrollment Protocol. The **HRA** is a **registration authority (RA)** which requests a health certificate from a certificate authority (CA) upon validation of health.

Health State: An abstract notion of the state of a machine used to indicate its compliance with network polices. Some examples of such state would include the state of the firewall on the machine, the version of the virus signature files for an antivirus application, and so on.

HexConvertedUnicodeString: A Unicode string created from a binary, byte-granular value. The string is created by converting each byte, starting with the most significant byte and ending with the least significant byte, into two Unicode characters. The characters are the hexadecimal representation of each nibble of the byte, starting with the high-order nibble.

Hibernation Image: An image containing metadata required to support a Windows operating system feature known as hibernation. Hibernation allows a system's state to be preserved in persistent storage while the system is shut down.

HMAC: See **Hash-based Message Authentication Code**.

Horizon: An integer parameter of the RDC FilterMax Algorithm. It refers to the number of consecutive hash values on both sides of a file offset.

Host: (1) The computer responsible for responding to DirectPlay game session enumeration requests and maintaining the master copy of all the player and group lists for the game. One computer is designated as the host of the DirectPlay game session. All other participants in the DirectPlay game session are called peers.

Host Bus Adapter (HBA): A host bus adapter that can be discovered via the SNIA Common HBA API on the system. For more information, see [HBAAPI].

Host Migration: Host migration is the process that occurs when the DirectPlay peer that is designated as the host leaves the DirectPlay game session, and the next oldest peer becomes the host. The algorithm employed during the host migration process is specified by the Host Migration Extension ([MC-DPLVP] section 1.3.2.1).

HRESULT: An opaque integer result value where the high bit indicates an error. Some protocols use only a constrained set of the HRESULT values where the only legal success value is 0x00000000. Any such protocols are responsible for documenting the fact that other success codes cannot be used.

HTTP Client: A program that establishes connections for the purpose of sending requests, as specified in [RFC2616].

HTTP Internal Server Error: An HTTP response with status code 500, as specified in [RFC2616], section 6.1.1.

HTTP OK: An HTTP response with status code 200, as specified in [RFC2616], section 6.1.1.

HTTP Proxy: An intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. For more information, see [RFC2616].

HTTP Server: An application that accepts connections in order to service requests by sending back responses. For more information, see [RFC2616].

Hypertext Transfer Protocol (HTTP): An application-level protocol for distributed, collaborative, hypermedia information systems (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS): An extension of HTTP that securely encrypts and decrypts Web page requests.

11 I

IDL: See **Interface Definition Language**.

IDTable: A table of File Replication Service (FRS) state information that contains an entry with version and identity information for each file and folder in the replica tree. It is used to keep track of all files in the replica set and their history.

Immediate Error Cause: An error in a protocol layer within a software agent that prevents the successful completion of a task in the same or different protocol layer/software agent. Any error resulting from such failure is also said to be caused by the **immediate error cause**.

Impersonation Level: The ability of an operating system process or thread to run temporarily in the security context of a specific caller and to gain authorized access to resources using that identity.

IN Channel: An inbound HTTP request or an inbound TCP/IP connection between two network nodes acting in one of the roles defined by this protocol. An IN channel is independent from the underlying transport and can be based on an HTTP or HTTPS request or on a TCP connection.

IN Channel Recycling: The set of mechanisms involved in closing an open IN channel **N** and opening a new IN channel **N+1**. The opening and subsequent closing occur as part of the sequence of channels forming a virtual **IN channel**.

Inbound: The network traffic flowing from the client to the server.

Inbound Connection: For a given replica member, a component of the **NTFRS member** object in Active Directory that identifies **inbound partners**. An **inbound connection** exists for each **inbound partner**.

Inbound Log: A queue storing pending change orders to be processed. As entries in the queue are processed, acknowledgments are sent to the **inbound partners**.

Inbound Partner: The partner that sends out change orders, files, and folders.

Inbound Proxy: A network node that acts as proxy for inbound traffic between a client and a server.

Inbound Trust: A state in which the **trusted domain** trusts the **primary domain** to perform operations such as name lookups and authentication.

Incoming Authentication: A mode in which each party (the reference party) verifies the identity of the other party, as specified in [RFC3748] section 7.2.1, but not vice-versa.

INF file: A file providing Windows Setup with the information required to set up a device, such as a list of valid logical configurations for the device and the names of driver files associated with the device.

Information Level: A number used to identify the volume, file, or device information being requested by a client. Corresponding to each **information level**, the server returns a specific structure to the client that contains different information in the response.

Inheritance: See **Object Class Inheritance**.

Initial Sync: The process that a new member to the replica set has to go through before it is allowed to synchronize with its outbound partners. Also called vvjoin.

Initiator: The party that sends the first message of an **IKE** exchange.

Inner EAP method: An **EAP method** that is tunneled within another EAP method.

In-Site: In-site targets. Two or more targets sharing the same namespace as a client.

Installation Files: Files referenced in the metadata of a software installation package. **Installation files** are used to install the software described by the software installation package on client computers.

IntegerConvertedUnicodeString: A Unicode string created from a binary value. The string is a representation of the integer interpretation of the binary value. For example, a value of 0x10 would be represented as the string "16".

Integrated Drive Electronics (IDE) Bus: A standard electronic interface used between a computer motherboard's bus and the computer's disk storage devices.

Interactive Logon: A software method in which the account information and credentials input by the user interactively are authenticated by a server or domain controller (DC).

Interface: (1) A specification in a COM server that describes how to access the methods of a class. For more information, see [MS-DCOM].

(2) A group of related function prototypes in a specific order, analogous to a C++ virtual interface. Multiple objects, of different object class, may implement the same interface. A derived interface may be created by adding methods after the end of an existing interface. In DCOM, all interfaces initially derive from **IUnknown**.

Interface Definition Language (IDL): The ISO standard language for specifying the interface for remote procedure calls. For more information, see section "Interface Definition Language" in Part 3 of [C706].

Interface Identifier (IID): A GUID that identifies an interface.

Interface Pointer: A pointer to an interface implemented by an [MS-DCOM] object.

Interface Pointer Identifier (IPID): A 128-bit number that uniquely identifies an interface on an object within an object exporter.

Internet Key Exchange (IKE): The protocol used to negotiate and provide authenticated keying material for security associations (SAs) in a protected manner. For more information, see [RFC2409].

Internet Protocol Security (IPsec): A framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks through the use of cryptographic security services. **IPsec** supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. The Microsoft implementation of **IPsec** is based on standards developed by the Internet Engineering Task Force (IETF) IPsec working group.

Internet SCSI (iSCSI): For terms related to **iSCSI**, see [RFC3720].

Internet Security Association and Key Management Protocol (ISAKMP): A cryptographic protocol specified in [RFC2408] that defines procedures and packet formats to establish, negotiate, modify and delete security associations (SAs). It forms the basis of the IKE protocol (as specified in [RFC2409]).

Internetwork Packet Exchange (IPX): A protocol maintained by Novell's NetWare product that provides connectionless datagram delivery of messages. The Internetwork Packet Exchange (IPX) is based on Xerox Corporation's Internetwork Packet protocol, XNS.

Inter-site Topology Generator: A domain controller (DC) within a given site that computes an NC replica graph for each NC replica on any domain controller (DC) in its site. This domain controller (DC) creates, updates, and deletes corresponding **nTDSConnection** objects for edges directed from NC replicas in other sites to NC replicas in its site.

Intrinsic Event: An event that defines an event generated by the implementation itself.

Invocation ID: A unique number that identifies the version of the directory database that is running on the domain controller (DC). Replication partners use the invocation ID and a Update Sequence Number (USN) to determine the most current changes for replication.

IPsec Administrative Plug-in: The **Internet Protocol security (IPsec)** extension plug-in that operates as part of the group policy configuration tool that reads and writes **IPsec** policy using the Group Policy: IP Security (IPsec) Protocol Extension.

IPsec Client-side Plug-in: The **IPsec** extension plug-in that operates on the client machine to retrieve the policy using the Group Policy: IP Security (IPsec) Protocol Extension.

IPsec Component: The implementation of the **IPsec**/**IKE** functionality on a client machine. This is the component that this Group Policy: IP Security (IPsec) Protocol Extension configures with the **IPsec**/**IKE** policy that is transferred as part of the protocol.

IPsec Group Policy Extension: The group policy extension protocol that transfers **IPsec**/**IKE** configuration information (like **IKE** settings, **IPsec** framing configuration and so on).

IPv4 Address in String Format: A string representation of an IPv4 address in the decimal dotted notation, as specified in [RFC1123] section 2.1.

IPv6 Address in String Format: A string representation of an IPv6 address as specified in [RFC4291] section 2.2.

IRemUnknown: An ORPC interface that contains methods used to call QueryInterface, AddRef, and Release on remote objects, as specified in [MS-DCOM].

IRemUnknown2: Extends the functionality of IRemUnknown, as specified in [MS-DCOM].

ISAKMP Payload: A modular building block for constructing **ISAKMP** messages. A payload is used to transfer information such as security association (SA) data, or key generation and authentication data. The presence and order of payloads in a packet is defined by and dependent upon the type of exchange specified in the **ISAKMP** header of the **ISAKMP** message. For more information, see [RFC2408] section 4.1.

iSCSI Initiator: For terms related to iSCSI Initiator, see [RFC3720].

iSCSI Initiator Adapter: For terms related to iSCSI Initiator Adapter, see [RFC3720].

iSCSI Initiator Portal: For terms related to iSCSI Initiator Portal, see [RFC3720].

iSCSI Session: For terms related to iSCSI Session, see [RFC3720].

ISO/OSI Reference Model: The International Organization for Standardization Open Systems Interconnection (ISO/OSI) reference model is a layered architecture (plan) that standardizes levels of service and types of interaction for computers that are exchanging information through a communications network. Also called OSI reference model.

Issuer Name: The name of the certificate authority (CA) that signed and issued a certificate. The name is an X.509 format name, as specified in [X509].

ISTG: See **Inter-site Topology Generator**.

IUnknown: An interface required in all COM and DCOM objects. This interface is required for controlling an object's lifetime and for dynamically querying for other interfaces supported by an object. For more information, see [MSDN-COM].

12 K

Kerberos: An authentication system that enables two parties to exchange private information across an otherwise open network by assigning a unique key (called a **ticket**) to each user that logs on to the network and then embedding these tickets into messages sent by the users. For more information, see [MS-KILE].

Kerberos Authenticator: A record sent with a ticket to a server to help certify the client's knowledge of the encryption key in the ticket, to help the server detect replay attacks by proving the authenticator is recently constructed, and to help the two parties select additional encryption keys for a particular connection authenticated by Kerberos. The use of authenticators, including how authenticators are validated, is specified in [RFC4120] section 5.5.1. For more information, see [KAUFMAN].

Kerberos Principal: A unique individual **account** known to the **key distribution center (KDC)**. Often a user, but it can be a service offering a resource on the network.

Key: (1) In the registry, a node in the logical tree of the data store.

(2) In cryptography, a generic term used to refer to cryptographic data that is used to initialize a cryptographic algorithm. Keys are also sometimes referred to as **keying material**.

Key Agreement: A key establishment procedure where the resulting secret keying material is a function of information contributed by two participants so that no party can predetermine the value of the secret keying material independently from the contributions of the other parties. See also, Key Transport. For more information, see section 3.1 in [SP800-56A] and in section 3 in [IEEE1363].

Key Archival: Also referred to as **key escrow**. The process by which the entity requesting the certificate also submits the private key during the process. The private key is encrypted such that only a **key recovery agent** can obtain it, preventing accidental disclosure, but preserving a copy in case the entity is unable or unwilling to decrypt data.

Key Archival Certificate: See **Key Recovery Certificate**.

Key Derivation: The act of deriving a cryptographic key from another value; for example, the derivation of a cryptographic key from a password.

Key Distribution Center (KDC): The Kerberos service that implements the authentication and ticket granting services specified in the Kerberos protocol. The service runs on computers selected by the administrator of the realm or domain; it is not present on every machine on the network. It must have access to an account database for the realm that it serves. Windows **KDCs** are integrated into the domain controller role of Windows 2000 Server or Windows Server 2003. It is a network service that supplies tickets to clients for use in authenticating to services.

Key Escrow: See **Key Archival**.

Key Establishment: See **Key Exchange**.

Key Exchange: A synonym for **key establishment**. The procedure that results in shared secret keying material among different parties. **Key agreement** and key transport are two forms of **key exchange**. For more information, see [CRYPTO] section 1.11, [SP800-56A] section 3.1, and [IEEE1363] section 3.

Key Exchange Key: The key used to protect the session key that is generated by the client. The **key exchange key** is derived from the response key during authentication.

Key Handle: The remote procedure call (RPC) context handle to a key.

Key Recovery Agent (KRA): A user, machine, or registration authority that has enrolled and obtained a **key recovery certificate**. A **KRA** is any entity that possesses a **KRA** private key and certificate. For more information on the **KRAs** and the archival process, see [MSFT-ARCHIVE].

Key Recovery Certificate: A certificate with the unique object identifier (OID) in the extended key usage extension for **key archival**.

Keyed Hash: A cryptographic hash computed over both a symmetric key and data, as specified in [RFC2617]. For more information, see [RFC2104].

Keyed Hash Message Authentication Code (HMAC): A symmetric keyed hashing algorithm used to verify the integrity of data to help ensure it has not been modified while in storage or transit.

Keyholder: The entity that holds a private key and is therefore capable of signing and decrypting. The keyholder of a public key is defined as the keyholder of the corresponding private key.

Keying Material: The data from which the main mode (MM) and quick mode (QM) security association (SA) authentication and encryption keys are generated.

Knowledge Consistency Checker (KCC): An internal Windows component of the Active Directory replication used to create spanning trees for DC-to-DC replication and to translate those trees into a set of abstract variables.

KRB_AP_REQ/KRB_AP_REP: The request and response messages used in the **AP exchange**.

KRB_AS_REQ/KRB_AS_REP: The request and response messages used in the Authentication Service (AS) Exchange.

KRB_CRED Exchange: The Kerberos sub-protocol used by clients requiring the ability to send credentials from one host to another. This exchange is initiated when a client sends a KRB_CRED message, as specified in [RFC4120] 3.6.

KRB_PRIV Exchange: The Kerberos sub-protocol used by clients requiring confidentiality and the ability to detect modifications of the messages they exchange with a server in a session already established through the AP exchange. This exchange is initiated when a client sends a KRB_PRIV message, as specified in [RFC4120] 3.5.

KRB_SAFE Exchange: The Kerberos sub-protocol used by clients to detect modifications of messages they exchange with a server in a session already established through the AP exchange. This exchange is initiated when a client sends a KRB_SAFE message, as specified in[RFC4120] 3.4.

KRB_TGS_REQ/KRB_TGS_REP: The request and response messages used in the **TGS exchange**.

13 L

LAN Adapter (LANA): A number used to identify a network adapter to which NetBIOS is bound.

LangID: See **Primary Language Identifier**.

Language Code Identifier (LCID): A 32-bit number that identifies the user interface human language dialect/variation supported by an application or client computer.

Language Identifier: See **Language Code Identifier (LCID)**.

Locale ID: See **Language Code Identifier (LCID)**.

LDAP: See **Lightweight Directory Access Protocol (LDAP)**.

LDAP Connection: A TCP connection from a client to a server over which the client sends LDAP protocol requests and the server sends responses to the client's requests.

Lightweight Directory Access Protocol (LDAP): The primary access protocol for Active Directory (as specified in [MS-ADTS]). **LDAP** is an industry-standard protocol, established by the Internet Engineering Task Force (IETF), which allows users to query and update information in a directory service (as specified in [MS-ADTS]). For more information, see [RFC2251].

Lingering Object: A domain controller (DC) that was offline for longer than the value of the **tombstone lifetime** can contain objects that have been deleted on other domain controllers (DCs) and for which tombstones no longer exist.

Link: When the value of an attribute refers to a directory object, and the attribute's Attribute-Schema object has an even value for attribute **linkId**, then that attribute value is a link. Sometimes referred to as a forward link.

Link Attribute: A **forward link attribute** or a back link attribute.

Link Order: An integer that describes the precedence of a Group Policy object (GPO) associated with an **SOM** compared to other Group Policy objects (GPOs) associated with that SOM.

Link Value: The value of a **link attribute**.

LinkValueStamp: The type of a stamp attached to a **link value**.

Listening State: A server or proxy state in which the server or proxy is able to accept and respond to events coming from the network.

Little-Endian: Multiple-byte values that are byte-ordered with the least significant byte stored in the memory location with the lowest address.

LM Hash: A DES-based cryptographic hash of a clear text password.

LMOWF: A general purpose function used in the context of NTLM authentication protocol, as specified in [MS-NLMP], that computes a one-way function of the user's password.

Local Area Network (LAN): A local computer network for communication between computers.

Local Change Order: A change order that is created because of a change to a file or folder on the local server. The local server becomes the originator of the change order and constructs a staging file.

Local Domain Controller (DC): A domain controller (DC) on which the current method is executing.

Local Master Browser: The browser on a given subnet that was elected to maintain the master copy of information related to a given domain. That is, different domains have different local master browsers on the same subnet.

Local Master Browser Server: A server that is elected master browser server on a particular subnet across a domain.

Local Maximum: A pair consisting of an offset "I" in a file and the hash value h(bi-Hash Window .. bi), that has the property that for all j ≥ 0 such that I - horizon ≤ j ≤ I + horizon, j = I OR h(bj-Hash Window .. bj) < h(bi-Hash Window .. bi), where for all k < 0, bk is defined to be 0. **Local maxima** are used to find deleted points by the RDC FilterMax algorithm.

Local Security Authority (LSA): A protected subsystem that authenticates and logs users onto the local system. **LSA** also maintains information about all aspects of local security on a system, collectively known as the **local security policy** of the system.

Local Security Authority (LSA) Database: A Microsoft-specific terminology for the part of the user account database containing account privilege information (such as specific account rights) and domain security policy information.

Local Security Policy: A collection of security settings present on a machine that affects how that machine regulates access to the resources it provides.

Localizable: Anything that is language or country specific.

Localizable Information: The portion of information in a CIM class definition that could be language or country specific.

Locally Unique Identifier (LUID): A 64-bit value guaranteed to be unique within the scope of a single machine.

Locator: (1) In remote procedure call (RPC), a component of the **Remote Procedure Call Name Service** that runs on a given machine and facilitates the name service operations of exports and lookups.

(2) In the context of domain controllers (DCs), the functionality encompassed by the DC Locator Protocol. Broadly, the cooperative function between clients and domain controllers (DCs), which allow clients to locate their nearest domain controller (DC) offering particular feature services.

Locked Partition: A partition that is inaccessible.

Logical Cluster Number (LCN): The cluster number relative to the beginning of the volume. The first cluster on a volume is zero (0).

Logical Connection: The state maintained on client and server in association with a connectionId.

Logical Disk Manager (LDM): A subsystem of Windows that manages dynamic disks. Dynamic disks contain a master boot record at the beginning of the disk, one **LDM** partition, and an **LDM** database at the end. The **LDM** database contains partitioning information used by the **LDM**.

Logical Drive: A set of disk extents that compose a volume.

Logical Partition: See **Logical Drive**.

Logical Unit Number (LUN): A number used to identify a disk on a given disk controller.

Lost and Found Container: A container holding objects in a given naming context (NC) that do not have parent objects due to add and remove operations that originated on different domain controllers (DCs). The container is a child of the naming context (NC) root and has RDN CN=LostAndFound in domain naming contexts (NCs) and CN=LostAndFoundConfig in Config naming contexts (NCs).

14 M

Machine: A reference to a physical device that replicates files.

Machine Account: An account associated with individual client or server machines in an Active Directory domain.

Machine Connection: A connection to a printer (shared from a print server) on a client machine. A connection is displayed in the user interface as a printer. **Machine connections** are displayed for all users (in all user environments) of a particular client machine.

Machine Group Policy Object (GPO) Version: A version number of the changes for the computer policy portion of a Group Policy object (GPO). This is a 16-bit integer encoded in the lower 16 bits of a GPO version.

Machine Identifier: A GUID that is unique for each machine.

MachineID: A unique identifier that represents the identity of a computer.

Mailslot:

1. A mechanism for one-way interprocess communications (IPC). For more information, see [MSLOT] and [MS-MAIL].

2. Within the NetBIOS protocol, refers to the datagram style of communication.

Mailslot Class: An indication of the expected service of the **mailslot**. Class 1 is guaranteed delivery, and class 2 is not guaranteed delivery.

Main Mode (MM): The first phase of an IKE negotiation that performs authentication and negotiates a **main mode security association (MM SA)** between the peers. For more information, see [RFC2409] section 5.

Main Mode Security Association (MM SA): A security Association used to protect IKE traffic between two peers. For more information, see [RFC2408] section 2.

Main Stream: The place within a file where data is stored, or the data stored therein. A **main stream** has no name. The **main stream** is what is ordinarily thought of as the contents of a file.

Manageable Entity: A CIM instance representing a manageable component of an operating system.

Mandatory TLV: An attribute that is required in an SoH or SoHR message in order for that message to be valid and complete.

Man in the Middle (MITM): An attack that deceives a server or client into accepting an unauthorized upstream host as the actual legitimate host. Instead, the upstream host is an attacker's host that is manipulating the network so the attacker's host appears to be the desired destination. This enables the attacker to decrypt and access all network traffic that would go to the actual legitimate host.

Marshal: To encode one or more data structures into an octet stream using a specific remote procedure call (RPC) transfer syntax. For example, marshaling a 32-bit integer.

Marshaling: The act of formatting COM parameters for transmission over remote procedure call (RPC). For more information, see [MS-DCOM].

Masked Disk: A disk that is invisible to the local machine, even though a physical connection exists between the disk and the machine.

Mass Storage Device: Any hardware device that provides persistent storage of data.

Master Boot Record (MBR): Metadata such as the partition table, the disk signature, and executable code for initiating the operating system boot process that is located on the first sector of a disk. Disks that have **MBRs** are referred to as **MBR** disks. GUID Partitioning Table (GPT) disks, instead, have unused dummy data in the first sector where the **MBR** would normally be.

Master Browser Server: A server responsible for maintaining a master list of available resources on a subnet, and for making the list available to backup browser servers. Each subnet requires a **master browser server**. The **master browser server** for a particular domain is called the domain master browser server.

Master Locator: Enables querying for server entries exported on a different machine.

Master Session Key: A temporary cryptographic key used to derive other cryptographic keys to be used to encrypt and decrypt parts of session-based protocol.

Maximum Transmission Unit (MTU): The size, in bytes, of the largest packet that a given layer of a communications protocol can pass onward.

MD5 Hash: A hashing algorithm, as specified in [RFC1231] that was developed by RSA Data Security, Inc. An **MD5 hash** is used by File Replication Service (FRS) to verify that a file on each replica member is identical.

Member (DFS-R): A computer participating in replication.

Member Server: A server joined to a domain and that is not acting as an Active Directory domain services domain controller (DC).

Merge Disks Or Disk Groups: The act of combining disks in two separate and distinct disk groups to form a single disk group.

Message: See **Message Tag (MTAG)**.

Message Authentication Code (MAC): A message authenticator computed through the use of a symmetric key.

Message Authentication Code (MAC) Protocol Data Unit (MPDU): The unit of data exchanged between two peer **message authentication code (MAC)** entities by using the services of the physical layer.

Message Authentication Code (MAC) Sublayer Management Entity (MLME): An entity that provides the layer management service interfaces through which layer management functions may be invoked.

Message Digest: See Hash Function.

Message Digest 4 (MD4): As specified in [RFC1320], a collision-resistant, non-rolling hash function that produces a 16-byte hash. While **MD4** is no longer considered to be cryptographically secure, RDC does not rely on cryptographic security in its hash function.

Message Identifier: An index into a message table. A message table is a collection of localizable strings. For Windows implementations, the message table is stored in the resource section of a dynamic link library.

Message Mode: A Named Pipe can be of two types: byte mode or **message mode**. In byte mode, the data sent or received on the Named Pipe does not have message boundaries but is treated as a continuous Stream. In Message Mode, message boundaries are enforced.

Message Server: An remote procedure call (RPC) server that implements this protocol.

Message Tag (MTAG): A message that is sent between participants in the context of connections.

Messaging Application Programming Interface (MAPI): A Windows programming interface that enables you to send e-mail from within a Windows application.

Microsoft Interface Definition Language (MIDL): The Microsoft implementation and extension of **OSF-DCE** Interface Definition Language (IDL). **MIDL** can also mean the IDL compiler provided by Microsoft. For more information, see [MS-RPCE].

Microsoft Management Console (MMC): The Microsoft Management Console (MMC) provides a framework that consists of a graphical user interface (GUI) and a programming platform in which snap-ins (collections of administrative tools) can be created, opened, and saved. MMC is a multiple-document interface (MDI) application.

Mirrored Volume: A fault-tolerant volume that maintains two or more copies of the volume's data. In the event a disk is lost, at least one copy of the volume's data remains and can be accessed.

Mixed Mode: A state of an Active Directory domain that supports domain controllers (DCs) running Windows NT Server 4.0. **Mixed mode** does not allow organizations to take advantage of new Active Directory features such as universal groups, nested group membership, and inter-domain group membership.

Mixed Proxy: A network node that acts as a proxy for both inbound and outbound traffic between a client and a server.

Modification Sequence Number: An implementation-defined value for objects such as disks, volumes, drive letters, partitions and regions that increases monotonically each time a configuration operation takes place on the object.

Managed Object Format (MOF): While [DMTF-DSP004] defines a textual encoding for CIM objects called managed object format (MOF), this representation is not used within protocol operations defined in [MS-WMI]. The MOF text encoding is only used for illustrative purposes. The binary encoding in this specification can be translated to and from the MOF format.

Most Specific Object Class: The class that none of the other classes inherits from, in a sequence of object classes related by inheritance. The special object class top is less specific than any other class.

Mount Path: See **Mounted Folder**.

Mount Point: See **Mounted Folder**.

Mount Point Access Path: See **Mounted Folder**.

Mounted Folder: A file system directory that contains a linked path to a second volume. A user may link a path on one volume to another, for example given to volumes C: and D:, a user can create a directory or folder C:\mountD and link that directory with volume D:. The path C:\MountD can then be used to access the root folder of volume D:.

MSZIP Compression Algorithm: The compression algorithm implementing RFC 1591 that is used between Windows 2000 domain controllers (DCs). For more information, see [RFC1591].

Multipartition Volume: A volume containing data that exists on more than one partition.

Multiplexed Request: A request where client server message block (SMB) requests from various applications and users are all sent over the same SMB transport connection.

Mutual Authentication: A mode in which each party verifies the identity of the other party, as specified in [RFC3748] section 7.2.1.

15 N

Name Service Entry: A unit of advertisement exported to the RPC Name Service. These entries are of three types: a Server Entry, which contains bindings for a single server and optionally a set of Object UUIDs (for more information, see [C706], section "Name Service Attributes"); a Group Entry, which contains names of one or more server entries, other groups, or both (for more information, see [C706], section "Name Service Attributes"); and a Profile Entry, which contains a prioritized set of profile elements (for more information, see [C706], section "Name Service Attributes").

Name Service Provider Interface (NSPI): A method of performing address-book-related operations on Active Directory.

Name Table: The list of systems participating in a DXDiag session that are employed for both local use and for transmission to enable peer-to-peer connectivity when additional participants join. This could also be considered the player list. It has a version number that monotonically increases with every operation that changes the name table content, such as adding or removing a player.

Named Pipe: A named, one-way, or duplex pipe for communication between a pipe server and one or more pipe clients.

Named Stream: A place within a file in addition to the main stream where data is stored, or the data stored therein. File systems support a mode in which it is possible to open either the main stream of a file, and/or to open a **named stream**. **Named streams** have different data than the main stream (and than each other), and may be read and written independently. Not all file systems support **named streams**. See also, main stream.

Naming Context (NC): A dsname, containing at least a DN and a GUID, used in forming names for a tree of objects. The DN of the dsname is the **distinguishedName** attribute of the tree root. The GUID of the dsname is the **objectGuid** attribute of the tree root. The SID of the dsname, if present, is the **objectSid** attribute of the tree root. The SID is present if and only if the **naming context (NC)** is a domain NC. Active Directory allows **naming contexts (NCs)** to be arranged into a tree structure.

Naming Context (NC) Replica: A tree of objects whose root object is identified by the **naming context**, which is a dsname.

Naming Context (NC) Replica Graph: A directed graph containing **naming context (NC)** replicas as nodes and repsFrom tuples as inbound edges by which originating updates replicate from each full replica of a given **naming context (NC)** to all other **naming context (NC)** replicas of the **naming context (NC)**, directly or transitively.

Naming Context Root (NC Root): The specific directory object referenced by the **naming context** dsname.

NAP: See **Network Access Protection**.

Native Mode: A state of an Active Directory domain in which all current and future domain controllers (DCs) run Windows 2000 Server or higher; no domain controllers (DCs) run Windows NT Server 4.0. **Native mode** allows organizations to take advantage of new Active Directory features such as universal groups, nested group membership, and inter-domain group membership.

NBNS: Net Bios Name Service.

NC: See **Naming Context**.

Negotiation: A series of exchanges. The successful outcome of a **negotiation** is the establishment of one or more SAs. For more information, see [RFC2408] section 2.

Negotiation Discovery: An IKE extension that improves interoperation between Internet Protocol security (IPsec) and non-IPsec-aware hosts. Detecting that the peer host is not capable of IPsec usually involves waiting for the IKE negotiation to time out, then sending traffic in the clear. With **negotiation discovery**, the host starts the IKE negotiation and sends clear text traffic in parallel. If the IKE negotiation succeeds and SAs are established, further traffic is secured.

Negotiation Filter Association (NFA): The logical binding of the appropriate IPsec Filter and IPsec Negotiation Policy settings together for an IPsec policy.

NetBIOS: A particular network transport that is part of the LAN Manager protocol suite. **NetBIOS** uses a broadcast communication style that was applicable to early segmented local area networks. The LAN Manager protocols were the default in Windows NT environments prior to Windows 2000.

NetBIOS Datagram Service: An implementation of **NetBIOS** services in a datagram environment as specified in section 17 of [RFC1001].

NetBIOS Name: A 16-byte address that is used to identify a **NetBIOS** resource on the network. For more information, see [RFC1001] and [RFC1002].

Netlogon: In a Windows NT-compatible network security environment, the component responsible for synchronization and maintenance functions between a primary domain controller (PDC) and backup domain controllers. **Netlogon** is a precursor to the DRS protocol.

Network Access Policy: A set of rules that determines the behavior of a **network access server (NAS)**. The policy consists of a set of conditions that matches an access request to the policy and an access profile.

Network Access Protection (NAP): A feature of an operating system that provides a platform for system health-validated access to private networks. **NAP** provides a way of detecting the health state of a network client that is attempting to connect to or communicate on a network, and limiting the access of the network client until the health policy requirements have been met.

Network Access Protection (NAP) Client: A computer that supports the **Network Access Protection** feature by complying with the corresponding policy settings.

Network Access Protection (NAP) Group Policy (GP) Extension GUID: A GUID defined separately for each computer policy setting that associates a specific administrative tool extension with a set of policy settings that can be stored in a Group Policy object (GPO).

Network Access Server (NAS): A computer server that provides an access service for a user to a network. A **network access server (NAS)** operates as a client of **RADIUS**. The **RADIUS client** is responsible for passing user information to designated RADIUS servers, and then acting on the response returned by the RADIUS server. Examples of an NAS include: a VPN server, Wireless Access Point, 802.1x-enabled switch, or **Network Access Protection (NAP)** server.

Network Address Translation (NAT): The process of converting between IP addresses used within an intranet, or other private network, and Internet IP addresses.

Network Byte Order: The order in which the bytes of a multiple-byte number are transmitted on a network, most significant byte first (in big-endian storage). This may or may not match the order in which numbers are normally stored in memory for a particular processor.

Network Data Representation (NDR): A specification that defines a mapping from Interface Definition Language data types onto octet streams. **NDR** also refers to the runtime environment that implements the mapping facilities (for example, data provided to **NDR**). For more information, see [MS-RPCE] and chapter 14 of [C706].

Network Logon: A software method in which the account information and credentials previously supplied by the user as part of an interactive logon are used again to log the user onto another network resource.

Network Redirector: A software component on a connected computer that handles requests for remote files and printer operations.

NT File System (NTFS): The native file system for Windows 2000 and later versions. For more information, see [MSFT-NTFS].

Node: A computer system that is configured as a member of a cluster. That is, the computer has the necessary software installed and configured to participate in the cluster, and the cluster configuration includes this computer as a member.

Nonce: A number that is used only once. This is typically implemented as a random number large enough that the probability of number reuse is vanishingly small. A **nonce** is used in authentication protocols to prevent replay attacks. For more information, see [RFC2617].

Non-Replicated Attribute: An attribute whose values are not replicated between **naming context (NC)** replicas. The non-replicated attributes of an object are, in effect, local variables of the domain controller (DC) hosting the **naming context (NC)** replica containing that object, since changes to these attributes have no effect outside that domain controller (DC).

Normal Sync: The synchronization among replicas after initial sync is done.

Notification Area: An area of the desktop's **taskbar** containing program icons that provide status and notifications on events and system state, such as incoming e-mail messages, updates, and network connectivity.

Notification Icon: An icon placed in the notification area.

NT Backup File: A file that contains the representation of another file. It is made up of zero or more backup streams.

NT Hash: An MD5-based cryptographic hash of a clear text password. For more information, see [MS-NLMP].

nTDSDSA object: An object of class nTDSDSA, representing a domain controller (DC) in the Config **naming context (NC)**.

NTFRS Member: Each NTFRS member object (class nTFRSMember) corresponds to a computer that is part of a replica set.

NTFRS Object: An Active Directory object of class nTFRSMember.

NTFS: See **NT File System (NTFS)**.

NT LAN Manager Protocol (NTLM): A protocol using a challenge-response mechanism for authentication in which clients are able to verify their identities without sending a password to

the server. It consists of three messages, commonly referred to as Type 1 (negotiation), Type 2 (challenge) and Type 3 (authentication). For more information, see [MS-NLMP].

NTOWF: A general purpose function used in the context of NTLM authentication protocol, as specified in [MS-NLMP], which computes a one-way function of the user's password. For more information, see [MS-NLMP] section 7.

NULL GUID: A GUID of all zeros.

16 O

Object: (1) A set of attributes, each with its associated values. Two attributes of an object have special significance:

- Identifying attribute: A designated single-valued attribute appears on every object; the value of this attribute identifies the object. For the set of objects in a replica, the values of the identifying attribute are distinct.
- Parent-identifying attribute: A designated single-valued attribute appears on every object; the value of this attribute identifies the object's parent. That is, this attribute contains the value of the parent's identifying attribute, or a reserved value identifying no object. For the set of objects in a replica, the values of this parent-identifying attribute define a tree with objects as vertices and child-parent references as directed edges with the child as an edge's tail and the parent as an edge's head.

Note that an object is a value, not a variable; a replica is a variable. The process of adding, modifying, or deleting an object in a replica replaces the entire value of the replica with a new value.

As the word replica suggests, it is often the case that two replicas contain "the same objects." In this usage, objects in two replicas are considered "the same" if they have the same value of the identifying attribute and if there is a process in place (replication) to converge the values of the remaining attributes. When the members of a set of replicas are considered to be the same, it is common to say "an object" as shorthand referring to the set of corresponding objects in the replicas.

(2) In Active Directory, an entity consisting of a set of attributes, each attribute with a set of associated values. For more information, see [MS-ADTS].

(3) In COM, an instance of an object class. Each object implements one or more interfaces that may be obtained from each other using the **IUnknown** interface.

(4) A DCOM object, as specified in [MS-DCOM] section 1.1.

Object Class: (1) A predicate defined on objects which constrains their attributes. Also an identifier for such a predicate.

(2) A set of restrictions on the construction and update of objects. An **object class** can specify a set of must-have attributes (every object of the class must have at least one value of each) and may-have attributes (every object of the class may have a value of each). An **object class** can also specify the allowable classes for the parent object of an object in the class. An **object class** can be defined by single-inheritance; an object whose class is defined in this way is a member of all **object classes** used to derive its most specific class. An **object class** is defined in a **classSchema** object.

Object Class Inheritance: The process of defining one **object class** in terms of its variations from an existing **object class**. The may-have, must-have, and possible superiors restrictions of an **object class** are all inherited.

Object Class Name: The lDAPDisplayName of the **classSchema** object of an **object class**. The correspondence between LDAP display names and numeric **object identifiers (OIDs)** is specified in [MS-ADTS].

Object Exporter: An object container (for example, process, machine, thread) in an object server. **Object exporters** are callable using RPC interfaces, and they are responsible for dispatching calls to the objects they contain.

Object Exporter Identifier (OXID): A 64-bit number that uniquely identifies an **object exporter** within an object server.

Object ID: See **ObjectID**.

Object Identifier (OID): (1) In the context of an object server, a 64-bit number that uniquely identifies an object.

(2) In the context of a directory service, a number identifying an object class or attribute. Object identifiers are issued by the ITU and form a hierarchy. An object identifier is represented as a dotted decimal string (for example, "1.2.3.4"). For more information on OIDs, see [X660] and Appendix A of [RFC3280]. **OIDs** are used to uniquely identify certificate templates available to the certificate authority (CA). Within a certificate, **OIDs** are used to identify standard extensions as covered in section 4.2.1.x of [RFC3280] as well as non-standard extensions.

(3) In LDAP, a sequence of numbers in a format specified by [RFC1778]. In many LDAP directory implementations, an **OID** is the standard internal representation of an attribute. In the directory model used in this specification, the more familiar ldapDisplayName represents an attribute.

(4) In the context of **Abstract Syntax Notation One (ASN.1)**, an object identifier, as specified in [ITUX680].

(5) A variable-length identifier from a namespace administered by the ITU. Objects, protocols, and so on, that make use of ASN.1 or BER, DER, or CER encoding format leverage identities from the ITU. For more information, see [ITUX680].

Object of Class X (or X Object): An object **o** such that one of the values of its **objectClass** attributes is **x**. For instance, if **objectClass** contains the value **user**, **o** is an object of class **user**. This is often contracted to "user object".

Object Reference: An attribute value that references an object. Reading a reference gives the distinguished name (DN) of the object. An object reference allows the object to be accessed by entities outside the object's exporter.

Object Resolver: A service in an object server that supports instantiating objects, obtaining RPC binding information for object exporters, and managing object lifetimes. **Object resolvers** may be reachable via well-known or dynamic RPC endpoints.

Object Remote Procedure Call (ORPC): A remote procedure call whose target is an interface on an object. The target interface (and hence object) is identified by an **IPID**.

Object Server: An execution environment that contains a particular object resolver service and its associated object exporters.

Object UUID: A UUID used to represent a resource available on the RPC Servers. For more information, see [C706].

ObjectClass: The attribute on an object that holds an identifier for each object class of an object.

objectGuid: (1) The attribute on an object whose value is a GUID that uniquely identifies the object. The value of **objectGuid** is assigned when an object is created and is immutable thereafter. The integrity of both object references between naming contexts (NCs) and of replication depends on the integrity of the **objectGuid** attribute.

(2) The GUID of an Active Directory (AD) object. For more information, see [MS-ADTS].

ObjectID: A unique identifier that represents the identity of a file within a file system volume. For more information, see [MS-DLTM].

objectSid: The attribute on an object whose value is a security identifier (SID) that identifies the object as a security principal object. The value of objectSID is assigned when a security principal object is created and is immutable thereafter. The integrity of authentication depends on the integrity of the objectSid attribute.

OBJREF: The **marshaled** form of an object reference.

OEM Character: See **Original Equipment Manufacturer (OEM) Character**.

OEM Character Set: See **Original Equipment Manufacturer (OEM) Character Set**.

OEM Code Page: See **Original Equipment Manufacturer (OEM) Code Page**.

Offline: An operational state applicable to volumes and disks. In the offline state, the volume or disk is unavailable for data I/O or configuration.

OID: See **Object Identifier**.

OleTx: A comprehensive distributed transaction manager processing protocol that uses the [MS-CMPO], [MS-CMP], [MS-DTCM], and[MS-CMOM] protocols.

One-Way Authentication: An authentication mode in which only one party verifies the identity of the other party.

One-Way Function (OWF): The calculation of a hash of the password using the RSA MD4 function. **OWF** is used to refer to the resulting value of the hash operation.

Online: An operational state applicable to volumes and disks. In the online state, the volume or disk is available for data I/O or configuration.

Operating System Upgrade: The action of replacing the existing operating system on a computer with a later version of the operating system, while maintaining the original configuration and data of that computer.

Operational Attribute: An attribute returned only when requested by name in an LDAP search request. An LDAP search request requesting "all attributes" does not return operational attributes and their values.

Opportunistic Lock (Oplock): A mechanism designed to allow clients to dynamically alter their buffering strategy in a consistent manner to increase performance and reduce network use. The network performance for remote file operations may be increased if a client can locally buffer file data, which reduces or eliminates the need to send and receive network packets. For example, a client may not have to write information into a file on a remote server if the client knows that no other process is accessing the data. Likewise, the client may buffer read-ahead data from the remote file if the client knows that no other process is writing data to the remote file.

There are three types of **Oplocks**:

Exclusive Oplock allows a client to open a file for exclusive access and allows the client to perform arbitrary buffering.

Batch Oplock allows a client to keep a file open on the server even though the local accessor on the client machine has closed the file.

Level II Oplock indicates that there are multiple readers of a file and no writers. Level II Oplocks are supported if the negotiated SMB Dialect is NT LM 0.12 or later.

When a client opens a file, it requests the server to grant it a particular type of **Oplocks** on the file. The response from the server indicates the type of **Oplocks** granted to the client. The client uses the granted **Oplocks** type to adjust its buffering policy.

Oplock Break: An unsolicited request sent by an server message block (SMB) server to an SMB client to inform the client to change the **Oplock** level for a file.

Opnum: An operation number or numeric identifier used to identify a specific RPC method or method in an interface. For more information, see [C706] section 12.5.2.12 or [MS-RPCE].

Optical Media Drive: A drive that controls the positioning, reading, and writing of removable media on optical disks such as CD-ROMs and DVDs.

Oriented Tree: A directed acyclic graph such that for every vertex v, except one (the root), there is a unique edge whose tail is v. There is no edge whose tail is the root. For more information, see [KNUTH1], section 2.3.4.2.

Original Equipment Manufacturer (OEM) Character: An eight-bit encoding used in MS-DOS and Windows operating systems to associate a sequence of bits with specific characters. The ASCII character set maps the letters, numerals, and specified punctuation and control characters to the numbers from 0 to 127. The term "code page" is used to refer to extensions of the ASCII character set that map specified characters and symbols to the numbers from 128 to 255. These code pages are referred to as OEM Character sets. For more information, see [MSCHARSET].

Original Equipment Manufacturer (OEM) Character Set: A character encoding used where the mappings between characters is dependent upon the code page configured on the machine, typically by the manufacturer.

Original Equipment Manufacturer (OEM) Code Page: A code page used to translate between non-Unicode encoded strings and UTF-16 encoding strings.

Originating Update: An update performed to an NC replica directly by a client, as opposed to an update applied by replication from another NC replica. An **originating update** to an attribute or link value generates a new stamp for the attribute or link value.

Originating Write: An update operation that should be replicated to other replicas. The **originating write** is changing the server state. The inputs of the operation are the DSNAME of the object, the old value of replication metadata, and the list of modified attributes and values. The result of the operation is the new replication metadata stamped on the object.

Originator GUID: A GUID that is associated with each replica member. All change orders produced by a given replica member carry the replica member's originator GUID, which is saved in the IDTable. The **Originator GUID** is not the same as member GUID, which is the objectGuid of the NTFRS member object in Active Directory. For more information, see [MS-ADTS].

ORPC Extension: An out-of-band (not part of the explicit method signature), GUID-tagged binary large object (BLOB) of data that is sent or received in an ORPC call.

OSF-DCE: The Distributed Computing Environment from the Open Software Foundation. It consists of multiple components, including remote procedure call (RPC), which have been integrated to work closely together.

OUT Channel: An outbound HTTP response or an outbound TCP/IP connection between two network nodes acting in one of the roles defined by a protocol. An OUT channel is independent from the underlying transport and can be based on an HTTP or HTTPS response or on a TCP connection.

OUT Channel Recycling: The set of mechanisms involved in closing an open OUT channel N and opening a new OUT channel N+1. The opening and subsequent closing occur as part of the sequence of channels forming a virtual OUT channel.

Outbound: Network traffic flowing from the server to the client.

Outbound Connection: For a given replica member, a component of the NTFRS member object in Active Directory that identifies outbound partners. An **outbound connection** exists for each outbound partner.

Outbound Log (OutLog): A table in the File Replication Service(FRS) database that stores pending change orders to be sent to outbound partners. The changes can originate locally or come from an inbound partner. These change orders are eventually sent to all outbound replica partners.

Outbound Partner: The partner that receives change orders, files, and folders.

Outbound Proxy: A network node that acts as proxy for outbound traffic between a client and a server.

Outbound Trust: The primary domain trusts the trusted domain to perform operations such as name lookups and authentication.

Out-of-Band Policy Application: A protocol exchange between a client and server in which policy enforcement occurs for some subset of Group Policy settings from Group Policy objects (GPOs) encountered during some previous policy application exchange. This is referred to as out-of-band because, unlike policy application, out-of-band policy application retrieves settings separately from GPO retrieval.

OXID Resolution: The process of obtaining the RPC binding information required to communicate with the object exporter.

17 P

Pack: See Disk Group.

PackageRegistration Object: An Active Directory container that represents a software installation extension setting. The container is an object of class **groupPolicyContainer**, as specified in [MS-ADSC] section 56).

Packet Marking: The act of filling out a special value, such as a **DSCP** value, on individual packets, as specified in [RFC2474].

Padding: Bytes that are inserted in a data stream to maintain alignment of the protocol requests on natural boundaries.

Page Description Language (PDL): The language for describing the layout and contents of a printed page. Common examples are PostScript and **Printer Control Language (PCL)**.

Page File or Paging File: A file used by operating systems for managing virtual memory.

Parent GUID: The GUID of the parent folder that contains a particular file or folder in the replica tree.

Parent Object: An object is either the root of a tree of objects or has a parent. If two objects have the same parent they must have different values in their RDNs. See also, **Object**.

Partial Attribute Set (PAS): The subset of attributes that replicate to partial naming context (NC) replicas. Also, the particular partial attribute set that is part of the state of a forest, and used to control the attributes that replicate to global catalog (GC) servers.

Partial Database Synchronization: A mechanism for synchronizing a set of database records on a particular replication partner.

Partial Replica: A naming context (NC) replica that contains a schema-specified subset of attributes for the objects it contains. A partial replica is not writable as it does not accept originating updates.

Partition: A logical region of a hard disk. A hard disk may be subdivided into one or more **partitions**.

Partition Table: An area of a disk used to store metadata information about the **partitions** on the disk. See also, GUID Partitioning Table (GPT).

Partition Type: A value indicating the **partition's** intended use, or indicating the type of file system on the **partition**. For example, **partition** type 0x07 indicates that the **partition** is formatted with the NTFS file system. Original equipment manufactures may designate a **partition** type of 0x12 to indicate that manufacturer specific data is stored on the **partition**.

Partner: A computer connected to a local computer through either inbound or outbound connections.

Password Policy: A set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly.

Path: When referring to a file path on a file system, a hierarchical sequence of folders. When referring to a connection to a storage device, it is a connection through which a machine can communicate with the storage device.

Paused: A service that is not available because it has been placed in a suspended state, usually as a result of explicit administrative action.

PDC: See **Primary Domain Controller**.

PDU: See **Protocol Data Unit**.

PDU Stream: An ordered sequence of RPC and RPC over HTTP **protocol data units**.

Peak Rate: A value in a TSpec used to specify an aspect of network traffic behavior, as specified in [RFC2212].

Peer: (1) The entity being authenticated by the authenticator.

>(2) In **DirectPlay**, a peer refers to a player within a DirectPlay game session that has an established connection with every other peer in the game session, and which is not performing game session management duties. The participant that is managing the game session is called the host.

Peer-to-Peer Mode: A game playing mode that consists of multiple peers. Each peer has a connection to all other peers in the DirectPlay game session. If there are N peers in the game session, then each peer has N–1 connections.

Perfect Forward Secrecy (PFS): A property of key exchange protocols, which holds when session keys from previous communications are not compromised by the disclosure of longer term keying material. In the context of Internet Protocol security (IPsec), **PFS** requires a Diffie-Hellman exchange to generate the keys for each quick mode (QM) security association (SA).

Permission X on Object Y: An access check where the access type is X and the security descriptor is read from object Y's LDAP attribute securityDescriptor.

Phase: A series of exchanges providing a particular set of security services (for example, authentication or creation of security associations (SAs)).

Phase I Authentication Set: A collection of settings that specifies how Internet Protocol security (IPsec) performs phase I (or main mode) authentication.

Phase I Cryptographic Set: A collection of settings that specifies how Internet Protocol security (IPsec) performs phase I (or main mode) key exchange.

Phase I Cryptographic Suite: One or more phase I cryptographic suites are associated with a phase I cryptographic set. Each phase I cryptographic suite contains a Diffie-Hellman algorithm, an encryption algorithm, and an integrity algorithm.

Phase II Authentication Method: One or more phase I authentication methods are associated with each phase I authentication set. Each phase I authentication method specifies an authentication credential and in some cases additional information about how the authentication credential is used.

Phase II Authentication Set: A collection of settings that specifies how Internet Protocol security (IPsec) performs AuthIP extended mode authentication.

Phase II Cryptographic Set: A collection of settings that specifies how Internet Protocol security (IPsec) performs phase II (or quick mode) data protection.

Phase II Cryptographic Suite: One or more phase II cryptographic suites are associated with each phase II cryptographic set. Each phase II cryptographic suite contains a protocol

specifying how the packet is modified by Internet Protocol security (IPsec), an encryption algorithm, an integrity algorithm, and information about how frequently to regenerate the keys used to protect the data.

Phase One: The initial phase of a two-phase commit sequence. During this phase, the participants in the transaction are requested to prepare to be committed. This phase is also known as the "Prepare" phase. At the end of phase one, the outcome of the transaction is known.

Phase Two: The second phase of a two-phase commit sequence. This phase occurs after the decision to commit or abort is determined. During this phase, the participants in the transaction are ordered to either commit or rollback.

Ping: In the DC Locator protocol, a client sends a ping request to a domain controller (DC) in order to determine its responsiveness. When a client is actively soliciting the attention of a domain controller (DC), it is said to be pinging the domain controller (DC).

Ping Set: A set of DCOM objects on a particular object server in use by a particular client. The set is grouped in order to maintain the lifetimes of object references collectively for the set rather than individually for each object.

Ping Set Identifier (SETID): A 64-bit number that uniquely identifies a ping set within an object server.

Pinging: The process by which a client periodically contacts an object server to maintain the lifetime of its references to objects on that object server.

Pipe Instance: A request to open a named pipe by a client application. Multiple SMB clients can open the same named pipe. Each request to open the same named pipe is a **pipe instance**.

Pipe State: A series of attributes that describe how the pipe interacts with processes for various I/O operations and indicate how much data is currently available to be read from the named pipe.

Plaintext: In cryptography, ordinary readable text before being encrypted into ciphertext or after being decrypted.

Player: Represents a person that is playing a computer game. There may be multiple players on a computer participating in any given game session. See also **Name Table**.

Plex: See **Volume Plex**.

Plug a Channel: The act of switching a channel from **unplugged channel mode** to **plugged channel mode**.

Plugged Channel Mode: A channel mode in which an IN channel or OUT channel instance queues **protocol data units (PDUs)** instead of sending them immediately.

Policies Path: A domain-based Distributed File System (DFS) path for a directory on the server that is accessible through the SMB protocol. This path MUST be a path of the form \\<dns domain name>\sysvol\<dns domain name>\policies.

Policy: (1) The set of rules that govern the interaction between a subject and an object or resource.

(2) A collection of settings that contains global settings, profile settings, firewall rules, and connection security rules. Together these settings specify how the host firewall and Internet Protocol security (IPsec) behave on the client computer.

Policy Application: The protocol exchange by which a client obtains all of the Group Policy object (GPO) and thus all applicable Group Policy settings for a particular policy target from the server, as specified in [MS-GPOL]. Policy application can operate in two modes, user policy and computer policy.

Policy Setting: A statement of the possible behaviors of an element of a domain member computer's behavior that can be configured by an administrator.

Policy Target: A user or computer account for which policy settings can be obtained from a server in the same domain, as specified in [MS-GPOL]. For user policy mode, the policy target is a user account. For computer policy mode, the policy target is a computer account.

PostScript: A **Page Description Language** developed by Adobe Systems, it is primarily used for printing documents on laser printers. It is the standard for desktop publishing.

Potential Browser Server: A browser server that is capable of being a backup or master browser server, but is not currently fulfilling either of those roles.

Pre-Authentication: In Kerberos, allows a KDC to demand that the requestor in the AS Exchange demonstrate knowledge of the key associated with the account before the KDC will issue a ticket-granting ticket, or TGT, as specified in [RFC4120] sections 5.2.7 and 7.5.2.

Predecessor Channel: In the context of IN channel recycling or OUT channel recycling, the previous IN channel or OUT channel (–1 where N is the reference point) in the sequence of channels forming a virtual IN channel or virtual OUT channel.

Predecessor Inbound Proxy: An inbound proxy to which a predecessor channel was established.

Predecessor Outbound Proxy: An outbound proxy to which a predecessor channel was established.

PREDEFINED_KEY: Root keys that can be referenced by using well-known names and conforms to the tree structure.

Prefix Table: A data structure used to translate between an object identifier (OID) and a compressed representation for object identifiers (OIDs).

Primary Disk Group: In the context of dynamic disk, it is the disk group whose disks are online, which means they are accessible for I/O and configuration. Each machine may have only one primary disk group. Disks on the machine belonging to other disk groups are referred to as 'foreign disks' and their disk group is referred to as a 'foreign disk group.'

Primary Domain: A domain (identified by a security identifier (SID)) that the server is joined to. For a domain controller (DC), the **primary domain** is that of the domain itself.

Primary Domain Controller (PDC): A master domain controller (DC) that performs authentication on access requests from workstations and other servers, and manages information concerning network security and resources.

Primary Domain Controller (PDC) Role Owner: The domain controller (DC) that hosts the **primary domain controller** emulator FSMO role for a given domain naming context (NC).

Primary Group: The POSIX standard mandates that every Unix user be assigned a primary group ID (GID) as part of their identity. Setting this value for a user assigns the primary group as the POSIX primary GID when connecting to POSIX compliant applications.

Primary Language Identifier: The lower 10 bits of a language identifier. It identifies the user interface human language supported by an application or client computer without regard to variations such as dialect.

Primary Partition: A type of partition on an master boot record (MBR)-formatted disk.

Principal: (1) An authenticated entity that initiates a message or channel in a distributed system.

(2) An ID of such an entity.

(3) In Kerberos, a Kerberos principal.

Principal Name: The computer or user name maintained and authenticated by active directory (AD).

Principal Self: A **well-known SID** used to represent the identity of a security principal when that security principal is also the object that is being protected with a security descriptor. Applicable only to directory objects that are representing security principals, the principal self identifier allows the security descriptor on the directory object to grant specific user rights to the principal itself. As an example, a user object for fred@domain.com might have a security descriptor that allowed principal-self:update-shoe-size. The intent is to allow fred to update his own shoe size. The use of the fixed value SID for Principal Self prevents every user object from needing a unique security descriptor, thus conserving space in the directory database.

Principal's Secret Key: In Kerberos, a symmetric encryption key shared between an entity and the KDC, with a long lifetime and for the purpose of authentication. A password is a common example of a **principal's secret key**.

Print Client: The application or user trying to apply an operation on the print system either by printing a job or managing the data structures or devices maintained by the print system.

Printer Driver: The interface component between the operating system and the printer device. It is responsible for processing the application data into a **page description language (PDL)** that can be interpreted by the printer device.

Print Job: The rendered **page description language (PDL)** output data sent to a print device for a particular application or user request.

Print Queue: The logical entity to which jobs may be submitted for a particular print device. Associated with a print queue is a print driver, a user's print configuration in the form of a DEVMODE structure, and a system print configuration stored in the system registry.

Print Server: A machine that hosts the print system and all its different components.

Print System: A system component responsible for coordinating and controlling the operation of print queues, print drivers, and print jobs.

Printer Control Language (PCL): A **page description language (PDL)** developed by Hewlett Packard for their laser and ink-jet printers.

Printer Form: A preprinted blank paper form, or a print job's virtual representation of this form, that enables a printer to position form elements in their physical location on the page.

Private Key: One of a pair of keys used in public-key cryptography. The private key is kept secret and is used to decrypt data that has been encrypted with the corresponding public key. For an introduction to this concept, see [CRYPTO] section 1.8 and [IEEE1363] section 3.1.

Privilege: (1) The right of a user to perform system-related operations, such as debugging the system. A user's authorization context specifies what privileges are held by that user.

(2) The capability of a security principal to perform a type of operation on a computer system regardless of restrictions placed by discretionary access control.

Privilege Attribute Certificate (PAC): A Microsoft-specific authorization data present in the authorization data field of a ticket. The **PAC** contains several logical components, including group membership data for authorization; alternate credentials for non-Kerberos authentication protocols; and policy control information for supporting interactive logon.

Process Identifier (PID): A number used by some operating systems (for example, Windows and UNIX) to uniquely identify a process. For more information, see [PROCESS].

Product Identifier GUID: A unique identifier in the form of a GUID for the application described by a software installation package. Two such packages with the same product identifier GUID describe the same application.

Profile: A grouping of settings that is applied based on the network location of connected interfaces on the client computer. There are three profiles supported by Windows Firewall with Advanced Security: domain (used when connected to a corporate environment, private (used when connected to a home or small business behind a gateway device), and public (used when connected to a public hotspot such as a coffee shop or airport).

Profile Element: A record that corresponds to a single remote procedure call (RPC) interface and that refers to a server entry, group or profile. For more information, see [C706], section "Name Service Attributes."

Property: A data field within a CIM class definition. This consists of a simple name, a type, and a value.

Property Set: A set of attributes, identified by a GUID. Granting access to a property set grants access to all the attributes in the set.

Protected Attribute: A sensitive protected attribute that is not readable outside the LSA running on a domain controller (DC).

Protected Subsystem: The part of a system that is isolated from the rest of the system such that it cannot be affected by the non-protected parts of the system.

Protocol Data Unit (PDU): Information that is delivered as a unit among peer entities of a network and that may contain control information, address information, or data. See [C706] section 12 for more information.

Protocol Dialect: A protocol version that is distinct and non-interoperable from other protocol versions from the same group of related protocols.

Protocol Extension: An implementation-specific extension to a transaction manager that provides an implementation of a transaction processing protocol that the transaction manager does not implement natively.

Protocol Identifier: A numeric value that uniquely identifies an RPC transport protocol when describing a protocol in the context of a protocol tower. For more information, see [C706], section Protocol Identifiers.

Protocol Role: A class of protocol functionality that is identified as such for the purposes of a specification.

Protocol Sequence Identifier: A numeric value that uniquely identifies an RPC transport protocol when describing a protocol in the context of a protocol tower. For more details, see [C706-AppendixIProtocolID].

Protocol State: Information stored by a protocol that affects its behavior.

Protocol Tower: A protocol sequence along with its related address and protocol-specific information. For more information, see [C706] section Remote Procedure Call Model.

Protocol Type: A special set of standardized rules that endpoints in a communications connection use when transferring data.

Prototype Context: A context sent as part of an activation request.

Proxy: A network node that accepts network traffic originating from one network agent and transmits it to another network agent.

Pseudo-Random Number Generator (PRNG): An algorithm that generates values (numbers, bits, and so on) that give the appearance of being random from the point of view of any known test. If initialized with a true random value (called its "seed"), the output of a cryptographically strong PRNG will have the same resistance to guessing as a true random source.

Public Key: One of a pair of keys used in public-key cryptography. The public key is distributed freely and published as part of a digital certificate. For an introduction to this concept, see [CRYPTO] section 1.8 and [IEEE1363] section 3.1.

Public Key Algorithm: An asymmetric cipher that uses two cryptographic keys: one for encryption, the public key, and the other for decryption, the private key. In signature and verification, the roles are reversed: public key is used for verification, and private key is used for signature generation. Examples of public key algorithms are described in various standards, including DSA (Digital Signature Algorithm) and ECDSA (Elliptic Curve Digital Signature Algorithm) in FIPS 186-2 (as specified in [FIPS186]), RSA in PKCS#1 (as specified in [PKCS1]), NIST also published an introduction to public key technology in SP800-32 (as specified in [SP800-32]).

Public Key Cryptography Standards (PKCS): A group of Public Key Cryptography Standards published by RSA Laboratories.

Public Key Infrastructure (PKI): The laws, policies, standards, and software that regulate or manipulate certificates and public and private keys. In practice, it is a system of digital certificates, certification authorities, and other registration authorities that verify and authenticate the validity of each party involved in an electronic transaction. For more information, see section 6 of [X509].

Public-Private Key Pair: The association of a public key and its corresponding private key when used in cryptography. For an introduction to public-private key pairs, see section 3 in [IEEE1363].

Published Application: An application that should not be automatically installed at computer startup or user logon unless it is a required upgrade of an application that is installed on the computer. However, software maintenance applications on the computer can display information about this software and install or uninstall it, often at the direction of a user.

18 Q

Qualifier: A metadata item as specified in [DMTF-DSP0004] section 4.5.4. This consists of a simple name, a type, and a value, and a flavor (a propagation rule for the qualifier).

Quality of Service (QoS): A set of technologies that do network traffic manipulation, such as packet marking and reshaping.

Quick Format: A formatting that does not zero the data sectors on the volume at the time the file system metadata is created.

Quick Mode (QM): The second phase of an IKE negotiation during which the peers negotiate quick mode security associations (**quick mode security association (QM SA)**). For more information, see [RFC2409] section 5.5.

Quick Mode Security Association (QM SA): A security association (SA) used to protect IP packets between peers (the IKE traffic is protected by the main mode security association (MM SA)). For more information, see [RFC2409] section 5.5.

19 R

RADIUS Attribute: An abstract identifier for a value or set of values that describe elements of a RADIUS protocol exchange. RADIUS attributes describe the details of an endpoint's connection request and provides configuration data for a network access server (NAS) to provide service to the endpoint.

RADIUS Client: A client that is responsible for passing user information to designated RADIUS servers, and then acting on the response that is returned.

RADIUS Server: A server responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user. A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

RAID-0: A **RAID** volume that stripes its data across multiple **RAID columns**. Also called a striped volume.

RAID-1: See **Mirrored Volume**.

RAID-5: A fault-tolerant volume that maintains the volume's data across multiple **RAID columns**. Fault tolerance is provided by writing parity data for each stripe. In the event that one disk encounters a fault, that disk's data may be reconstructed using the parity data located on the other disks.

RAID Column: A **RAID** construct for organizing disks and volumes.

Raw Read (on a Named Pipe): The act of reading data from a named pipe that ignores message boundaries even if the pipe was set up as a message mode pipe.

Raw Write (on a Named Pipe): The act of writing data into a named pipe where the data must contain the message boundaries if the pipe is a message mode pipe. The operation can allow a single write to insert multiple messages.

RC4: A variable key-length **symmetric encryption** algorithm. For more information, see [SCHNEIER] section 17.1.

RDC FilterMax Algorithm: The algorithm that **RDC** uses to determine the deleted points in a File. The FilterMax algorithm has the property that it will often find deleted points that result in identical chunks being found in differing files, even when the files differ by insertions and deletions of bytes, not simply by length-preserving byte modifications.

RDN: The name of an object relative to its parent. This is the leftmost attribute-value pair in the DN of an object. For instance, in the DN "cn=Peter Houston, ou=NTDEV, dc=microsoft, dc=com", the RDN is "cn=Peter Houston". For more information, see [RFC2251].

RDN Attribute: The attribute used in an **RDN**. In the RDN "cn=Peter Houston" the **RDN attribute** is **cn**. In Active Directory, the **RDN attribute** of an object is determined by the most specific structural object class of the object.

Read Permission: Authorization to read an attribute of an object. For more information, see [MS-ADTS].

Read-Only: An attribute of storage media that denotes the media is not available to be written.

Read-Only Domain Controller (RODC): A domain controller (DC) that has a read-only copy of the given domain.

Read-Only Replicated Folders: Replicated folders where local changes are not replicated out and reverted by replicating back previous content.

Realm: (1) An administrative boundary that uses one set of authentication servers to manage and deploy a single set of unique identifiers. A realm is a unique login space.

(2) A collection of KDC, with a common set of principals, as specified in [RFC4120] 1.2.

Receive Window: The amount of memory a recipient of network traffic has committed to queuing protocol data unit (PDU) that it cannot process immediately.

Recovery: The process of re-establishing connectivity and synchronizing views on the outcome of transactions between two participants after a transient failure. Recovery occurs either between a resource manager and a transaction manager, or between a Superior Transaction Manager Facet and a Subordinate Transaction Manager Facet.

Recursion Level: For very large files, even the signature file may be large. In order to reduce the bandwidth needed to transfer signature files, **RDC** may be used in order to reduce the number of bytes that must be moved from server to client to transfer the signature file. This process may be repeated a number of times, producing successively smaller signature files. The recursion level is the number of times it is repeated. The first signature file is recursion level 1. The source data file is referred to as being at recursion level 0.

Redeploy Action: An action that an administrator may take for an application deployed through the software installation extension protocol that will cause all clients that receive the application through the protocol to perform an installation of the application on the client if the application is already installed. This is used by administrators as a mechanism to update the application.

Redundant Arrays of Independent Disks (RAID): A set of disk-organization techniques designed to achieve high-performance storage access and availability.

Reference Count: An integer value used to keep track of a COM object. When an object is created, its reference count is set to 1. Every time an interface is bound to the object, its reference count is incremented; when the interface connection is destroyed, the reference count is decremented. The object is destroyed when the reference count reaches zero. All interfaces to that object are then not valid.

RefreshTime: The last time that information for an entry in the VolumeTable or FileTable has been refreshed by its VolumeOwner.

REG_KEY_OPTIONS: DWORD values used to indicate the type of the key.

REG_VALUE_TYPE: DWORD values used to indicate the format of the data associated with a value.

Region: See Disk Extent.

Region Flags: A set of values that describes the region's state or use.

Region's Status: The status of the region, such as whether the region is performing properly, or encountering disk faults.

Registration: See Certification.

Registration Authority (RA): (1) A generic term for a software module, hardware component or human operator thereof that enables a user or public key infrastructure (PKI) administrator

to perform various administration and operational functions as part of the certification or revocation process.

(2) The authority in a public key infrastructure (PKI) that verifies user requests for a digital certificate and indicates to the certificate authority (CA) it is acceptable to issue a certificate.

Registry: A local system-defined database in which applications and system components store and retrieve configuration data. It is a hierarchical data store with lightly typed elements that are logically stored in tree format. Applications use the registry API to retrieve, modify, or delete registry data.

The data stored in the registry varies according to the version of Windows.

Registry Files: The physical representation of a logical tree in the registry.

Registry Policy File: A file associated with a Group Policy object (GPO) that contains a set of registry-based policy settings.

REGSAM: A bit field that specifies the user rights for a key object.

Relative Distinguished Name (RDN): (1) An attribute-value pair used in the distinguished name of an object. For more information, see [RFC2251].

(2) In Active Directory (AD), the unique name of a child element relative to its parent in AD. The RDN of a child element combined with the FQDN of the parent forms the FQDN of the child.

Relative Identifier (RID): The last item in the series of sub-authority values in a SID (as specified in [SIDS]). It distinguishes one account or group from all other accounts and groups in the domain. No two accounts or groups in any domain share the same relative identifier.

Release: The process of calling the third IUnknown method (IUnknown::Release()) on an object.

Reliable Time Source: A time source that can provide accurate time. It is usually the primary reference with stratum 1 as specified in [RFC1305]; for example, a radio clock.

Relying Party (RP): The entity (person or computer) using information from a certificate in order to make a security decision. Typically, the RP is responsible for guarding some resource and applying access control policies based on information learned from a certificate.

Remediation Server: A remediation server is a server responsible for bringing a noncompliant computer back into a compliant state.

Remote Application: An application running on a remote server.

Remote Authentication Dial-In User Service (RADIUS): A protocol for carrying authentication, authorization, and configuration information between a network access server (NAS) that prefers to authenticate connection requests from endpoints and a shared server that performs authentication, authorization and accounting.

Remote Access Service (RAS) Server: A type of NAS that provides modem dial-up or VPN access to a network.

Remote Administration Protocol (RAP): A synchronous, request/response protocol, used prior to the development of the Remote Procedure Call (RPC) protocol, for marshaling and unmarshaling procedure call input and output arguments into messages, and for reliably transporting messages to and from clients and servers.

Remote Change Order: A change order received from an inbound (or upstream) partner that originated elsewhere in the replica set.

Remote Desktop Protocol (RDP): The protocol used to implement remote connections (**Terminal Services**) on Windows operating systems. For more information, see [MSDN-RDP].

Remote Differential Compression (RDC): Any of a class of compression algorithms designed to compare two files residing on different machines without requiring one of the files to be transmitted in its entirety to the other machine.

Remote Procedure Call (RPC): A context-dependent term commonly overloaded with three meanings, defined below. Note that much of the industry literature concerning RPC technologies uses this term interchangeably for any of the three meanings. Below are the three definitions:

The runtime environment providing remote procedure call facilities. The preferred usage for this meaning is RPC runtime.

The pattern of request and response message exchange between two parties (typically, a client and a server). The preferred usage for this meaning is RPC exchange.

A single message from an exchange as defined in the previous definition. The preferred usage for this term is RPC message.

For more information see [C706].

Remote Procedure Call Name Service (RPC Name Service): A service that allows servers to export binding information, and clients to find it, in an efficient manner. For more information, see [C706], section "Name Service Interface".

Remote Server Name: A null-terminated Unicode string, supplied by an application, which in conjunction with an RPC protocol sequence is used to initiate communication with an object server.

Remote Unknown: An object exporter's remotely-accessible implementation of the IUnknown interface. Each object exporter has exactly one such remotely-accessible IUnknown implementation, which is responsible for handling all IUnknown invocations from clients.

Removable Media: A persistent storage device stores its data on media. If the media may be removed from the device then the media is considered removable. For example a floppy disk drive uses removable media.

Reparse Point: A collection of user-defined data associated with a file. The format of this data is understood by the application or the file system that stores the data, and the file system filter that interprets the data and processes the file. Reparse points can contain data that instructs the file system or the operating system to take special actions. For more information, see [MS-FSCC].

Replacement Channel: An IN channel or OUT channel other than the first in the sequence of IN Channels or OUT channels that constitute a virtual IN channel or virtual OUT channel.

Replica: (1) A variable containing a set of objects.

(2) FRS Replica: A member of a replica set. Replica contains machine-specific information.

(3) NC Replica: A replica of NC x is a tree of objects whose root object r satisfies dsname) = x.

Replica Set: (1) The representation of the replication group on a single computer. It is the slice of the replication group that affects the server that it exists on. For instance it contains only the connections where this computer is either the client or server.

(2) In FRS, the replication of files and directories according to a predefined topology and schedule on a specific folder. The topology and schedule are collectively called a replica set. A replica set contains a set of replicas, one for each machine that participates in replication.

Replica Tree: The local replica root folder together with all files and directories underneath it, which usually is saved as a tree structure in the file system.

ReplicaSetId: The GUID that is assigned to a specific replication group.

Replicated Attribute: An attribute whose values are replicated to other NC replicas. An attribute is replicated if its attributeSchema object o does not have a value for the systemFlags attribute or bit 0 of the value is clear.

Replicated Folder: Root of a replicated tree. All files and sub-folders (recursively) are replicated.

Replicated Update: An update performed to an naming context (NC) replica by the replication system, to propagate the effect of an originating write at another NC replica. The stamp assigned during the originating write to attribute values or a link value during is preserved by replication.

Replication: The process of propagating the effects of all originating writes, to any replica of an naming context (NC), to all replicas of the naming context (NC). If originating writes cease and replication continues, all replicas converge to a common application-visible state.

Replication Epoch: A state variable of a domain controller (DC) that changes when a domain controller (DC) is no longer compatible for replication with its former partners. A server receiving a replication request tests the client's replication epoch against its own, and refuses the request if the two are not equal.

Replication Group: A container for set of replicated folders sharing the same connections to replication partners.

Replication Latency: The time lag between a final originating update to an naming context (NC) replica and all naming context (NC) replicas reaching a common application-visible state.

Replication Session: The state maintained when replicating files in the context of a replicated folder and connection.

Replication Traffic: Network traffic performed to accomplish replication.

RequestMachine: The MachineID of the computer that is the client of the DLT Central Manager RPC protocol.

Requestor: The computer that sends the request messages that are defined by this protocol.

Reshaping: An act of buffering data until it can be sent in conformance to a TSpec, as specified in [RFC2212].

Reshaping Value: A value used for both the peak rate and the bucket rate in a TSpec to be used in reshaping.

Resource Group: A group object whose membership is added to the authorization context only if the server receiving the context is a member of the same domain as the resource group.

Responder: (1) The computer that responds to request messages.

(2) The party that responds to the first message of an AuthIP exchange.

(3) The party that responds to the first message of an IKE exchange.

Response Key: A key essentially derived from a one way hash of the password. It maybe calculated slightly differently based on what NTLM version is being used. It is then used to derive the key exchange key.

Retry Change Order: A change order that is in some state of completion but was blocked for some reason and must be retried later.

Revocation: The process of invalidating a certificate. For more details, see section 3.3 of [RFC3280].

RID: The last item in the series of sub-authority values in a SID. Differences in the RID are what distinguish the different SIDs generated within a domain. See also SID.

RID Allocation Pool: The set of RIDs that an NC replica can assign (to new objects with the objectSid attribute) without obtaining more RIDs from the RID available pool.

RID Available Pool: The set of RIDs for an NC that have not been assigned to the RID available pool of some replica of the NC. The RID available pool is represented by the values of attributes within the NC's RID Master FSMO role.

Rivest-Shamir-Adleman (RSA): A system for public key cryptography. **RSA** is specified in [RFC2437].

Role Change: The act of changing the role of a computer. The act of configuring a server to be a domain controller is called promotion. The act of configuring a domain controller to be a non domain controller server is called demotion.

Role: The domain role quantifies the relationship between a computer and a domain. domain roles include:

Joined - linked to a domain for purposes of policy and security

Standalone - not associated with any domain

Domain controller - linked to a domain, and hosting that domain

Role Separation: A concept of a certificate authority (CA) to enhance security by allowing a user to be assigned a single role such as auditor, backup manager, administrator and certificate manager. Role separation ensures that a user may not posses multiple roles at one time. Role separation is a common criteria requirement for the CIMC protection profile. For more information, see [CIMC-PP]. Not all CAs support role separation.

Rolling Hash Function: A hash function that can be computed incrementally over a set of data. Given an arbitrary integer n ≥ 0, some bytes b0 .. bn-1 and their hash h(b0..bn-1), a hash function h is a rolling hash function if one can compute h(b1 .. bn) in time that does not depend on n.

Root CA: (1) A type of certificate authority (CA) that is directly trusted by an end entity; that is, securely acquiring the value of a root CA public key requires some out-of-band steps. This term is not meant to imply that a root CA is necessarily at the top of any hierarchy, simply that the CA in question is trusted directly (as specified in [RFC2510]). A root CA is implemented in software and in Microsoft Windows, a root CA is the topmost CA in a CA

hierarchy (as specified in [MS-PKI]) and is the trust point for all certificates that are issued by the CAs in the CA hierarchy. If a user, computer, or service trusts a root CA, they implicitly trust all certificates that are issued by all other CAs in the CA hierarchy. For more information, see [RFC3280].

(2) Any certificate authority (CA) directly trusted by a relying party.

Root Certificate: A **self-signed certificate** that identifies the public key of a root **CA** and has been trusted to terminate a certificate chain.

Root Domain: (1) The domain that is created first in a forest.

(2) In Active Directory, The unique domain NC of an Active Directory forest that is the parent of the forest's Config NC. The Config NC's RDN is "cn=Configuration" relative to this parent.

Root DSE (rootDSE): The logical root of a directory server, whose DN is the empty string. In the LDAP protocol, the root DSE is a name-less entry (a DN with an empty string) containing the configuration status of the server. Typically access to this entry is available to unauthenticated clients. The root DSE contains attributes that represent the features, capabilities and extensions provided by the particular server.

Root Error: The last error in an error sequence.

rootDSE: See **Root DSE**.

RPC Client: A computer on the network that sends messages using RPC as its transport and waits for responses is the initiator in an RPC exchange.

RPC Context Handle: A representation of state maintained between an RPC client and server. The state is maintained on the server on behalf of the client. An RPC context handle is created by the server and given to the client. The client passes the RPC context handle back to the server in method calls to assist in identifying the state. For more information, see [C706].

RPC Dynamic Endpoint: A network-specific server address that is requested and assigned at run time. For more information, see [C706].

RPC Endpoint: A network-specific address of a server process for Remote Procedure Calls. The actual name of the RPC Endpoint depends on the RPC Protocol Sequence being used. For example, for the NCACN_IP_TCP RPC Protocol Sequence an RPC Endpoint might be TCP port 1025. For more information, see [C706].

RPC Engine: The runtime environment providing RPC facilities.

RPC over HTTP Proxy: A mixed proxy, inbound proxy or outbound proxy.

RPC PDU: A PDU originating in the RPC runtime. For more information on RPC PDUs see section "RPC PDU Encodings" in Part 4 of [C706] and section 2 of [MS-RPCE].

RPC Protocol Sequence: A character string that represents a valid combination of an RPC protocol, a network layer protocol, and a transport layer protocol. For more information, see [C706] and [MS-RPCE].

RPC Server: A computer on the network that waits for messages, processes them when they arrive, and sends responses using RPC as its transport acts as the responder during an RPC exchange.

RPC Session Key: See **Session Key**.

RPC Transfer Syntax: A method for encoding messages defined in an IDL file. RPC can support different encoding methods or transfer syntaxes. For more information, see [C706].

RPC Transport: The underlying network services used by the RPC runtime for communications between network nodes. For more information, see section "Introduction to the RPC API" in Part 2 of [C706].

RTS PDU: A **PDU** used to control communication settings on an IN channel or OUT channel, virtual IN channel or virtual OUT channel or virtual connection.

RTS Cookie: A 16-byte cryptographically strong random number exchanged between parties in an RPC over HTTP protocol sequence. RTS cookie has same uniqueness requirements as a UUID and implementations can use a UUID as the RTS cookie. An RTS cookie is used to reference virtual connections, IN channels, OUT channels and other protocol entities.

20 S

SAD: See **Security Association Database**.

Salt: An additional random quantity, specified as input to an encryption function that is used to increase the strength of the encryption.

Sanitized Name: The form of a certification authority (CA) name that is used in file names (such as for a certificate revocation list; see [MSFT-CRL] for more information) and in other contexts where character sets are restricted. The process of sanitizing the CA name is necessary to remove characters that are illegal for file names, registry key names, or distinguished name values, or that are illegal for technology-specific reasons.

SASL: The Simple Authentication and Security Layer, as specified in [RFC2222]. This is an authentication mechanism used by LDAP.

Schedule: The frequency at which data replicates.

Schema: The set of attributes and object classes that govern the creation and update of objects.

Schema Container: The root object of the schema NC.

Schema Naming Context (Schema NC): A specific type of NC, or an instance of that type. A forest has a single schema NC, which is replicated to each DC in the forest. No other NC replicas can contain these objects. Each attribute and class in the forest's schema is represented as a corresponding object in the forest's schema NC.

Schema Object: An object that defines an attribute or an object class. Schema objects are contained in the schema NC.

Scope of Management (SOM): An Active Directory site, domain, or organizational unit container. These containers contain user and computer accounts that can be managed through Group Policy. These scopes of management are themselves associated with GPOs, and the accounts within them are considered by the Group Policy protocol [MS-GPOL] to inherit that association.

Scoped Group Policy Object (GPO) Distinguished Name (DN): A **Group Policy Object (GPO) Distinguished Name (DN)** where the set of "CN=<cn>" elements is prepended with "CN=User" for the **User Policy Mode** of Policy Application and with "CN=Machine" for **Computer Policy Mode**.

Scoped GPO Path: A Group Policy object (GPO) path appended with "\User" for the user policy mode of policy application, and "\Machine" for computer policy mode.

Screen Coordinates: Coordinates relative to the top-left corner of the screen, which is at (0,0).

SCSI Logical Unit Number (LUN): See Logical Unit Number (LUN).

SCSI Port Number: A number that uniquely identifies a port on a SCSI disk controller. Each SCSI disk controller may support multiple SCSI bus attachments or ports for connecting SCSI devices to a computer.

SD: See **Security Descriptor**.

Secret Key: A symmetric encryption key shared by two entities, such as between a user and the domain controller, with a long lifetime. A password is a common example of a secret key. When used in a context that implies Kerberos only, a principal's secret key.

Secret Object: An element of the LSA Policy Database, which contains a value that is secret in that access to it is strictly controlled through cryptographic protections and restrictive access control mechanisms.

Sector: The smallest addressable unit of a disk.

Secure Channel: An authenticated RPC connection between two machines in a domain with an established security context used for signing and encrypting RPC packets.

Secure Desktop: Only trusted processes running as SYSTEM are allowed to run on the secure desktop.

Secure Sockets Layer (SSL): A security protocol that supports confidentiality and integrity of messages in client and server applications communicating over open networks. SSL uses two keys to encrypt data—a public key known to everyone and a private or secret key known only to the recipient of the message. SSL supports server and, optionally, client authentication using X.509 certificates (for more information, see [X509]). The SSL protocol is precursor to **Transport Layer Security (TLS)**. The TLS version 1.0 specification is based on SSL version 3.0.

Security Account Manager (SAM) Built-in Database: A Microsoft-specific terminology for the part of the user account database containing account information (such as account names and passwords) for accounts and groups pre-created at the database installation. See [SAM] for more information.

Security Association (SA): A simplex "connection" that provides security services to the traffic carried by it. See [RFC4301] for more information.

Security Association Database (SAD): A database containing parameters that are associated with each established (keyed) security association.

Security Context: (1) An abstract data structure containing authorization information for a particular security principal in the form of a collection of **SIDs**. One **SID** identifies the principal specifically, whereas others may represent other capabilities. A server uses the authorization information in a security context to check access to requested resources.

(2) An association of mutually established cryptographic keys with a key identifier.

Security Descriptor: A data structure containing the security information associated with a securable object. A security descriptor identifies an object's owner by **SID**.

If access control is configured for the object, its security descriptor contains a discretionary access control list (DACL) with SIDs for the security principals who are allowed or denied access. Applications use this structure to set and query an object's security status. The security descriptor is used to guard access to an object as well as control which type of auditing takes place when the object is accessed.

Security Identifier (SID): An identifier for security principals (in Windows, that is used to identify an account). Conceptually, the **SID** is composed of an account authority portion (typically a domain) and a smaller integer representing an identity relative to the account authority, termed the RID. The **SID** data type is defined in [MS-DTYP] section **2.4.2**. For more information, see [MS-SECO].

Security Policy: In the form of a collection of security policy settings, the policy itself is an expression of administrative intent regarding how computers and resources on their network should be secured.

Security Policy Database (SPD): A database specifying the policies that determine the disposition of all IP traffic inbound or outbound from a host or security gateway.

Security Policy Settings: Contained in security policies, the policy settings are the actual expression of how various security-related parameters on the computer are to be configured.

Security Principal: (1) A unique entity identifiable through cryptographic means by at least one key. Often corresponds to a human user, but also can be a service offering a resource to other security principals. Sometimes referred to simply as a principal.

(2) An identity that can be used to regulate access to resources, as specified in [MS-SECO]. A security principal can be a user, a computer, or a group that represents a set of users.

Security Principal Name (SPN): The name identifying a security principal. (for example, machinename$@domainname for a machine joined to a domain or username@domainname for a user. Domainname is resolved using the DNS system.)

Security Principal Object: An object that corresponds to a security principal. A security principal object contains an identifier, used by the system and applications to name the principal, and a secret shared only by the principal. In Active Directory, a security principal object has the objectSid attribute. In Active Directory, the user, computer, and group object classes examples of security principal object classes (though not every group object is a security principal object).

Security Protocol: A protocol that performs authentication and possibly additional security services on a network.

Security Provider: A pluggable security module that is specified by the protocol layer above RPC, and will cause RPC to use this module to secure messages in a communication session with the server. Sometimes referred to as an authentication service. For more information, see [C706] and [MS-RPCE].

Security Support Provider (SSP): A dynamic-link library (DLL) that implements the SSPI by making one or more security packages available to applications. Each security package provides mappings between an application's SSPI function calls and an actual security model's functions. Security packages support security protocols such as Kerberos authentication and the Microsoft LAN Manager.

Security Support Provider Interface (SSPI): A Windows-specific API implementation that provides the means for connected applications to call one of several security providers to establish authenticated connections and to exchange data securely over those connections. This is the Windows equivalent of GSS-API, and the two families of APIs are on-the-wire compatible.

Security Token: An opaque message or data packet produced by a GSS-style authentication package, and carried by the application protocol. The application has no visibility into the contents of the token.

Seed File or Seed Data: A file or files on the client used to supply data used in reconstructing the source file. RDC may use an arbitrary number of seed files in the process of copying a single source file. Sometimes called just "seed." Selecting seed files is implementation specific, but can be guided by using similarity traits.

Selective Single Master: Replication mode, where changes from only a single machine propagate to other machines.

Self-Signed Certificate: A certificate that is signed by its creator, and verified using the public key contained in it. Such certificates are also termed **root certificates**.

Semi-Synchronous Operation: An operation executed on the server side while the client is regularly checking if there is no response available from the server.

Sequence ID: A monotonically increasing 8-bit identifier for packets. This is typically represented as a field named **bSeq** in packet structures.

Serial Storage Architecture (SSA) Bus: Serial Storage Architecture (SSA) is a standard for high-speed access to high-capacity disk storage. An SSA bus is implemented to the SSA standard.

Serialize: See Marshal.

Server: (1) A computer on which the RPC server is executing.

(2) A replicating machine that sends replicated files to a partner (client). The terminology server alludes to the machine acting in response to requests from partners that want to receive replicated files.

Server Authentication: A mode of authentication in which only the server in the transaction proves its identity.

Server Challenge: A 64-bit nonce generated on the server side.

Server Group Policy Object (GPO) Distinguished Name (DN): A Group Policy Object (GPO) Distinguished Name (DN) that uses a specific server in the LDAP path syntax, as specified in [RFC2251], where the server name is a domain controller (DC) that is located as specified in [MS-NRPC] section 2.2.6.28.

Server Group Policy Object (GPO) Path: A Group Policy Object (GPO) Path where the Distributed File System (DFS) path contains a server name in the Distributed File System (DFS) path syntax, where the server name is a domain controller (DC).

Server Locator: Enables exporting of entries to Remote Procedure Call Name Service.

Server Message Block (SMB): A protocol used to request file and print services from server systems over a network. The Server Message Block (SMB) protocol extends the CIFS protocol with additional security, file, and disk management support. For more information, see [CIFS] and [MS-SMB].

Note Whenever SMB is indicated, SMB2 can also be included (unless otherwise stated).

Server Object: A class of object in the Config NC. A server object can have an nTDSDSA object as a child.

Server Role: The state of a domain controller, which can be one of two values—primary domain controller or backup domain controller.

Server-Scoped Group Policy Object (GPO) Distinguished Name (DN): A Scoped Group Policy object (GPO) distinguished name (DN) with a server name included in the path, as is the case for a Server GPO DN.

Server-Scoped Group Policy Object (GPO) Path: A Group Policy object (GPO) path with a server name included in the path, as is the case for a Server GPO Path.

Service: A process or agent available on the network, offering resources or services for clients. Examples of services include file servers, Web servers, and so on.

Service Account: A stored set of attributes representing a principal that provides a security context for services.

Service for User (S4U): Microsoft-specific extensions to the Kerberos protocol to allow a service to obtain a Kerberos service ticket for a user that has not authenticated to the KDC; includes S4U2proxy and S4U2self.

Service for User to Proxy (S4U2proxy): An extension that allows a service to obtain a service ticket on behalf of a user to a different service.

Service for User to Self (S4U2self): An extension that allows a service to obtain a Kerberos service ticket to itself. The service ticket contains the user's groups and can therefore be used in authorization decisions.

Service Principal: An entity that represents a service at the KDC. The service principal has a name and an associated key. A subclass of principal, a service principal generally does not correspond to a human user of the system, but rather an automated service providing a resource, such as a file server.

Service Principal Name (SPN): The name by which a client uniquely identifies an instance of a service for mutual authentication. See [SPNNAMES] for more information about SPN format and composing a unique SPN. Also see [RFC1964], section 2.1.1.

Service Provider: A module that abstracts details of underlying transports for generic DirectPlay message transmission. Each DirectPlay message is transmitted by a DirectPlay service provider. The service providers that shipped with DirectPlay 4 are modem, serial, IPX, and TCP/IP.

Service Set Identifier (SSID): A sequence of characters that names a wireless local area network (WLAN).

Service Ticket: A ticket for any service other than the Ticket Granting Service; serves only to classify a ticket as not a TGT or cross-realm (as specified in [RFC4120] section 1.2) TGT.

Session:

1. In Kerberos, an active communication channel established through Kerberos that also has an associated cryptographic key, message counters, and other state.
2. In SMB, a persistent-state association between an SMB client and SMB server. A session is tied to the lifetime of the underlying NetBIOS or TCP connection.
3. In CHAP, a session is a lasting connection between a peer and an authenticator.
4. In the Workstation service, an authenticated connection between two computers.
5. An active communication channel established through NTLM, that also has an associated cryptographic key, message counters, and other state.
6. In OleTx, an association of two partners that want to exchange messages.

Session Key: A relatively short-lived symmetric key. (A cryptographic key negotiated by the client and the server based on a shared secret.) A session key's lifespan is bounded by the session to which it is associated. A session key should be strong enough to withstand cryptanalysis for the lifespan of the session.

Session Layer: The fifth layer in the OSI architectural model as defined by the International Organization for Standardization (ISO). The session layer is used for establishing a communication session, implementing security, and performing authentication. The session layer responds to service requests from the presentation layer and issues service requests to the transport layer.

Session Security: The provision of message integrity and/or confidentiality to a session.

SHA1 Hash: A hashing algorithm as specified in [FIPS180-2] that was developed by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA).

Shadow Copy: A duplicate of data held on a volume at a well-defined instant in time.

Share: A resource offered by a CIFS server for access by CIFS clients over the network. A share typically represents a directory tree and its included files (referred to commonly as a "disk share" or "file share") or a printer (a "print share"). If the information about the share is saved in persistent store (for example, Windows registry) and reloaded when a file server is restarted then the share is referred to as sticky share. Some share names are reserved for specific functions and are referred to as special shares:

IPC$, reserved for interprocess communication.

ADMIN$, reserved for remote administration.

A$, B$, C$ (and other local disk names followed by a dollar sign), assigned to local disk devices

Share Connect: The act of establishing authentication and shared state between a CIFS server and client that allows a CIFS client to access a share offered by the CIFS server.

Shell: Part of the Microsoft Windows user interface (UI) that organizes and controls user access to a wide variety of objects necessary for running applications and managing the operating system. The most numerous are the folders and files that reside on computer storage media. There are also a number of virtual objects such as network printers and other computers. The Shell organizes these objects into a hierarchical namespace, and provides an API to access them.

Shell Link: A data object that contains information used to access another object in the Shell's namespace—that is, any object visible through Microsoft Windows Explorer. The types of objects that can be accessed through Shell links include files, folders, disk drives, and printers. A Shell link allows an application to access an object from anywhere in the namespace. The application does not need to know the current name and location of the object.

Shell Shortcut: A Shell link that has a shortcut icon; however, the terms Shell link and Shell shortcut are often used interchangeably.

SID: See **Security Identifier**.

Signal: In OleTx, the act of communicating an event between facets inside a transaction manager.

Signature: A structure containing a hash and block chunk size. The hash field is 16 bytes, and the chunk size field is a 2 byte unsigned integer.

Signature File: A file containing the signatures of another (source) file. There is a simple header that identifies the type of the file as a signature file, the size of the header itself, and the RDC library version number. Following the header are the signatures from the source file in the order they are generated from the chunks.

Signing Certificates: The certificate that represents the identity of an entity (for example, a CA, a Web server or an S/MIME mail author) and is used to verify signatures made by the private key of that entity. For more information, see [RFC3280].

Similarity Data: Information about a file that can be used to determine an appropriate seed file to select to reduce the amount of data transferred. Similarity data can be computed in any implementation specific ways.

Similarity Traits: Similarity data consists of one or more traits. Each trait summarizes an independent feature of a file. The features are computed by taking min-wise independent hash functions of a file's signatures. Similarity traits are used in selecting seed files.

Simple Mail Transfer Protocol (SMTP): A TCP/IP protocol used in sending and receiving e-mail.

Simple Volume: A volume whose data exists on a single partition.

Single-Instance Storage (SIS): An NTFS feature that implements links with the semantics of copies for files stored on an NTFS volume. SIS uses copy-on-close to implement the copy semantics of its links.

Single-Phase Commit: An optimization of the Two-Phase Commit Protocol in which a transaction manager delegates the right to decide the outcome of a transaction to its only subordinate participant. This optimization can result in an In Doubt outcome.

Site: An Active Directory term that defines a set of one or more TCP/IP subnets, where the subnets have high connectivity, as measured in terms of latency (low) and bandwidth (high). By defining sites (represented by site objects) an administrator can easily configure Active Directory access and replication topology to take advantage of the physical network. When users log in, Active Directory clients find DCs that are in the same site as the user, or near the same site if there is no DC in the site. For more information, see [MS-ADTS].

Site Coverage: The set of sites for which a domain controller (DC) is responsible, as configured by the administrator.

Site DN: The distinguished name for an object in Active Directory that represents a site.

Site Object: An object of class site, representing a site.

Site of DC: The site object that is an ancestor of the DC's nTDSDSA object.

Site Settings Object: For a given site with site object s, its site settings object o is the child of s such that o is of class nTDSSiteSettings and the RDN of o is CN=NTDS site settings.

SKU: See **Stock Keeping Unit**.

Slow Sync: The nominator for a synchronization sub-protocol used to perform a consistency check between the databases of two partners.

Small Computer System Interface (SCSI) Bus: A standard for connecting peripheral devices to a computer. A SCSI bus is an implementation of this standard.

Smart Card: A portable device that is shaped like a business card and is embedded with a memory chip and either a microprocessor or some non-programmable logic. Smart cards are often used as authentication tokens and for secure key storage. Smart cards used for secure key storage have the ability to perform cryptographic operations with the stored key without allowing the key itself to be read or otherwise extracted from the card.

SMTP: See **Simple Mail Transfer Protocol**.

Snapshot: The point in time at which a shadow copy of a volume is made.

Software Installation Package or Package: A file that describes other files and metadata necessary to describe an application's executable files and state and to install that application.

Software Installation Package Modification: A file that allows an administrator to specify configuration for an application that is installed on the client through a software installation package.

Software Maintenance Utility: An application that allows users to perform software management activities such as installation, uninstallation, or inventory of applications available through the software installation extension.

Software Package Container DN: A DN of the form "CN=Packages,<ClassStore>" where <ClassStore> is a Class Store Container DN.

Software Package DN: A DN of the form "CN=<SoftwarePackageId>,CN=Packages,<ClassStore>", where <ClassStore> is a Class Store Container DN and <SoftwarePackageId> is a Curly Braced GUID String.

Software Scripts Path: A file system path to a directory with a path of the form "<ScopedGPOPath>\Applications", where <ScopedGPOPath> is a Scoped GPO path.

SoH Client: A synonym for **system health entity**.

Source File or Source Data: A file on a server that is to be copied by RDC. Sometimes referred to as "source."

Sparse File: A file that has regions of data containing all zeros and in which some of the zero regions do not have disk space allocated for them.

SMB Connection: A raw transport connection between an SMB client and SMB server. The SMB Connection is assumed to provide reliable in-order message delivery semantics. An SMB Connection can be established over any available SMB transport supported by both the SMB client and the SMB server. An SMB Connection is sometimes referred to as a Virtual Connection, as specified in [CIFS].

SMB Dialect: There are several different versions and subversions of the Server Message Block (SMB) Protocol. A particular version of the SMB protocol is referred to as an SMB Dialect. Different SMB Dialects can include both new SMB messages as well as changes to the fields and semantics of existing SMB messages used in other SMB Dialects. When an SMB client connects to an SMB server, the client and server negotiate the SMB Dialect to be used.

SMB Session: An authenticated user connection established between an SMB client and an SMB server over an SMB Connection. There can be multiple active SMB Sessions over a single SMB Connection. The Uid field in the SMB packet header distinguishes the various Sessions.

SPD: See **Security Policy Database**.

SPN: See **Service Principal Name**.

Spool File: A representation of application content data than can be processed by a print driver. Common examples are enhanced metafile format and XML paper specification. For more information, see [MSDN-META] and [MSDN-XMLP].

SRV Record: A particular type of information record in DNS. Domain Controllers advertise their capabilities by publishing SRV records in DNS.

SSL: See **Secure Sockets Layer (SSL)**.

SSL/TLS Handshake: The process of negotiating and establishing a connection protected by SSL or TLS. For more information, see [SSL3] and [RFC2246].

Staging File: The backup of the changed file or folder. It encapsulates the data and attributes associated with a replicated file or folder. By creating the staging file, FRS ensures that file data can be supplied to partners regardless of any activity that might prevent access to the original file. The staging files can be compressed to save disk space and network bandwidth during replication.

Stamp: Information describing an originating update by a DC. The stamp is not the new data value; the stamp is information about the update that created the new data value. A stamp is often called metadata, because it is additional information that "talks about" the conventional data values. A stamp contains the following pieces of information: The unique identifier of the DC that made the originating update, a sequence number characterizing the order of this change relative to other changes made at the originating DC, a version number identifying the number of times the data value has been modified, and the time when the change occurred.

Standalone CA: A CA that is not a member of a domain. For more information, see [MSFT-PKI].

Standalone Machine: A machine that is not a domain member or a domain controller.

Standard User: A user that does not have administrative rights defined in its token and is a member of the users group. Users are prevented from making accidental or intentional system-wide changes but can perform normal daily computer tasks.

State Machine: A model of computing behavior composed of a specified number of states, transitions between those states, and actions to be taken. A state stores information about past transactions as it reflects input changes from the startup of the system to the present moment. A transition (such as connecting a network share) indicates a state change and is described by a condition that would need to be fulfilled to enable the transition. An action is a description of an activity that is to be performed at a given moment.

There are several action types:

Entry Action: Performed when entering the state.

Exit Action: Performed when exiting the state.

Input Action: Performed based on the present state, and input conditions.

Transition Action: Performed when executing a certain state transition.

Statement of Health (SoH): A collection of data generated by a system health entity, as specified in [MS-SOH], which defines the health state of a machine. The data is interpreted by

a Health Policy Server, which determines whether the machine is healthy or unhealthy according to the policies defined by an administrator.

Statement of Health Response (SoHR): A collection of data that represents the evaluation of the Statement of Health (SoH) according to network policies, as specified in [MS-SOH].

Station (STA): Any device that contains an IEEE 802.11 conformant medium access control and physical layer (PHY) interface to the wireless medium (WM).

Station Management Entity (SME): In general, a station management entity (SME) is regarded as responsible for functions such as the gathering of layer-dependent status from the various layer management entities and setting the value of layer-specific parameters. An SME would typically perform such functions on behalf of general system management entities and would implement standard management protocols.

Stock Keeping Unit (SKU): A unique code that refers to a particular manufactured object or source of revenue. An SKU can refer to a retail product (software in a box that is sold through a channel), or a subscription program (such as MSDN), or an online service (such as MSN).

StoreMaster: The single agent responsible for performing certain updates to file-link information stored in VolumeTable and FileTable within an Active Directory Table (ADT). For more information on VolumeTable and FileTable, see [MS-DLT-CENTRALMANAGER].

Stream: A sequence of bytes written to a file on the NTFS file system. Every file stored on a volume that uses the NTFS file system contains at least one stream, which is normally used to store the primary contents of the file. Additional streams within the file may be used to store file attributes, application parameters, or other information specific to that file. Every file has a default data stream, which is unnamed by default. That data stream, and any other data stream associated with a file, may optionally be named.

Strict NDR/NDR64 Data Consistency Check: A set of related rules for data validation during processing of an octet stream.

Structural Class: See **Structural Object Class**.

Structural Object Class: An object class that is not an 88 object class and can be instantiated to create a new object.

Subkey: A child node in the logical tree of the hierarchical data store.

Subnet Site: The association of a site with a particular client, based on the client's IP address.

Subordinate Transaction Manager: A role taken by a transaction manager that is responsible for voting on the outcome of an atomic transaction. A subordinate transaction manager coordinates the voting and notification of its subordinate participants on behalf of its superior transaction manager. When communicating with those subordinate participants, the subordinate transaction manager acts in the role of superior transaction manager. The root transaction manager is never a subordinate transaction manager. A subordinate transaction manager has exactly one superior transaction manager.

SubRequest: A request within a SYNC_VOLUME or SEARCH request.

Successor Channel: In the context of IN channel recycling or OUT channel recycling, the next IN channel or OUT channel in the sequence of channels forming a virtual IN channel or virtual OUT channel (N+1 where N represents the reference point in the sequence).

Successor Inbound Proxy: An inbound proxy to which a successor channel is established.

Successor Outbound Proxy: An outbound proxy to which a successor channel is established.

Superclasses and Subclasses: Superclasses and subclasses are CIM classes. A subclass is derived from a superclass. The subclasses inherit all features of its superclass but can add new features or redefine existing ones. A superclass is the CIM class from which a CIM class inherits.

Superior Transaction Manager: A role taken by a transaction manager that is responsible for gathering outcome votes and providing the final transaction outcome. A root transaction manager can act as a superior transaction manager to a number of subordinate transaction managers. A transaction manager can act as both a subordinate transaction manager and a superior transaction manager on the same transaction.

Symmetric Algorithm: A cryptographic algorithm that uses one secret key that may be shared between authorized parties. The key must be kept secret between communicating parties. The same key is used for both encryption and decryption. For an introduction to this concept and terminology, see section 1.5 in [CRYPTO], section 3 in [IEEE1363], and section 3.1 in [SP800-56A].

Symmetric Encryption: An encryption method that uses the same cryptographic key to encrypt and decrypt a given message.

Symmetric Key: A secret key used with a cryptographic symmetric algorithm. The key needs to be known to all communicating parties. For an introduction to this concept, see section 1.5 in [CRYPTO].

Synchronous Operation: An operation that is executed on the server side while the client is waiting for the response message.

Syntax: See **Attribute Syntax**.

System Access Control List (SACL): An ACL that controls the generation of audit messages for attempts to access a securable object. The ability to get or set an object's SACL is controlled by a privilege typically held only by system administrators.

System Command: A message sent to a window or notification icon via its system menu, or via a keyboard shortcut. Common system commands include minimize, maximize, move, and so on.

System Directory: A directory containing system files comprising the operating system.

System Health Entity: The entity on a machine that can generate a Statement of Health (SoH) for the machine and consume the corresponding Statement of Health Response (SoHR).

System Menu: See Window Menu.

System Partition: A partition that contains the boot loader needed to invoke the operating system on the boot partition. A system partition must also be an active partition. It can but is not required to be the same partition as the boot partition.

System Volume (SYSVOL): A shared directory that stores the server copy of the domain's public files that must be shared for common access and replication throughout a domain.

21 T

Target File: A file on the client that is the destination of an RDC copy.

Taskbar: A window (anchored to an edge of the screen) that contains the Start button and buttons for all open programs.

Terminal Server: A computer on which **Terminal Services** is running.

Terminal Services: A service that allows delivery of Windows-based applications, or the Windows desktop itself, to various computing devices. When a user runs an application on **Terminal Server**, the application execution takes place on the server and only keyboard, mouse and display information is transmitted over the network. Each user sees only his or her individual session, which is managed transparently by the server operating system, and is independent of any other client session.

TGS Exchange: The Kerberos sub-protocol in which the Key Distribution Center (KDC) distributes a session key and a ticket for the service requested by the client, as specified in [RFC4120] section 3.3. This exchange is initiated when the client sends the KDC a KRB_TGS_REQ message.

Tick Count: In DirectPlay, the count from when the system was booted, in milliseconds.

Ticket: A record generated by the KDC that helps a client authenticate to a service. It contains the client's identity, a unique cryptographic key for use with this ticket (the session key), a time stamp, and other information, all sealed using the service's secret key. It only serves to authenticate a client when presented along with a valid authenticator.

Ticket-Granting Service (TGS): A service that issues **tickets** for admission to other services in its own domain or for admission to the ticket-granting service in another domain.

Ticket-Granting Ticket (TGT): A special type of **ticket** that can be used to obtain other **tickets**. The TGT is obtained after the initial authentication in the **AS exchange**; thereafter, the user does not need to present his credentials, but can use the TGT to obtain subsequent tickets.

Time Peer: A **time source** with which a **time provider** is synchronized. A **time provider** can have more than one time peer.

Time Provider: A component that a **time service** relies on to either obtain accurate time stamps (from network or hardware time sources) or to provide those time stamps to other computers over the network.

Time Service: A system service that implements support for synchronizing a computer's local time with a **time source**.

Time Source: A component that possesses a clock and makes the clock's time available to other components for synchronization. For more information, see "reference source" in [RFC1305].

TLN: See **Top Level Name**.

TLS: See **Transport Layer Security (TLS)**.

Token: A set of rights and privileges for a given user.

Tombstone: (1) A deleted object in the directory that remains in storage until a configured amount of time (the **tombstone lifetime**) has passed, after which the object is permanently

deleted. By keeping the tombstone in existence for the **tombstone lifetime**, the deleted state of the object is able to replicate.

(2) In DFS-R, an update pertaining to a file deletion.

Tombstone Lifetime: To avoid inconsistencies in object deletion, the **tombstone lifetime** is configured to be many times larger than the worst-case replication latency.

Tool Extension GUID or Administrative Plug-in GUID: A GUID defined separately for each of the user policy settings and computer policy settings that associates a specific administrative tool plug-in with a set of policy settings that can be stored in a Group Policy object (GPO).

Tooltip: A window displaying text that is created when the mouse is moved over a window or notification icon.

Top Level Name (TLN): The root namespace of a forest. For example, if the forest a.com contains the domains a.com, b.a.com, and c.a.com, the TLN would be a.com.

Topology: The structure of the connections between members.

Track: Any of the concentric circles on a disk platter over which a magnetic head (used for reading and writing data on the disk) passes while the head is stationary but the disk is spinning. A track is subdivided into sectors, upon which data is read and written.

Transaction: In OleTx, an **atomic transaction**.

Transaction Identifier: The GUID that uniquely identifies an atomic transaction.

Transaction Manager: The party that is responsible for managing and distributing the outcome of atomic transactions. A transaction manager is either a root transaction manager or a subordinate transaction manager for a specified transaction.

Transaction Propagation: The act of coordinating two transaction managers to work together on a single atomic transaction. When propagating a transaction to a transaction manager that is not already a participant in the transaction, that transaction manager plays the role of subordinate transaction manager to the originating transaction manager, which will play the role of superior transaction manager. When propagating a transaction to a transaction manager that is already a participant in the transaction, no new superior or subordinate relationship is established.

Transitive Trust: The state of two domains establishing trust through an intermediary domain. For example, if domain A trusts domain B, and domain B trusts domain C, then domain A may be configured to trust domain C through transitive trust.

Transmission Control Protocol (TCP): A protocol used with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. TCP handles keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

Transport Layer: The fourth layer in the OSI architectural model as defined by the International Organization for Standardization (ISO). The transport layer provides for transfer correctness, data recovery, and flow control. The transport layer responds to service requests from the session layer and issues service requests to the network layer.

Transport Layer Security (TLS): A security protocol that supports confidentiality and integrity of messages in client and server applications communicating over open networks. **TLS**

supports server and, optionally, client authentication by using X.509 certificates (as specified in [X509]). **TLS** is standardized in the IETF TLS working group.

Transport Mode: An IP encapsulation mechanism as specified in [RFC4301] that provides IPsec security for host-to-host communication.

Triple Data Encryption Standard (DES): A block cipher formed from the Data Encryption Standard (DES) cipher by using it three times.

Trust: The state of accepting another authority's statements for the purposes of authentication and authorization. If domain A trusts domain B, domain A will accept domain B's authentication and authorization statements for principals represented by security principal objects in domain B; for example, the list of groups to which a particular user belongs. As a noun, a trust is the relationship described above between two domains. A trust must be backed by a cryptographic key.

Trust Attributes: A collection of attributes that define different characteristics of a trust within a domain or a forest.

Trust Object: An object representing a **trust**.

Trust Path: In a graph of domain **trusts**, the path through the graph between two domains that are linked by transitive trust. For example, if domain A trusts domain B, and domain B trusts domain C, then the trust path is A->B->C.

Trust Root: A store within the computer of a relying party that is protected from tampering and in which the root keys of all root CAs are held. Those root keys are typically encoded within self-signed certificates and the contents of a trust root are therefore sometimes called root certificates.

Trust Secret: A pair of keys used to encrypt or sign sensitive protocol data between two trust authorities, such as domain controllers.

Trusted Domain: A domain that is trusted to make authentication decisions for security principals in that domain.

Trusted Domain Object (TDO): A collection of properties defining a trust relationship with another domain, such as direction (do we trust them—outbound, or do they trust us—inbound or both), trust attributes, name and security identifier of the other domain. For more information, see [MS-ADTS].

Trusted Forest: A forest that is trusted to make authentication statements for security principals in that forest. Assuming forest A trusts forest B, all domains belonging to forest A will trust all domains in forest B, subject to policy configuration.

Trusted Platform Module (TPM): A microcontroller that stores keys, passwords, and digital certificates typically affixed to the motherboard of a PC.

Trustee: The recipient, expressed as an SID, of an access control capability expressed in a security descriptor.

TSpec: A set of characteristics used to specify network traffic behavior, as specified in [RFC2212].

Tunnel: The encapsulation of one network protocol within another.

Tunnel Mode: An IP encapsulation mechanism, as specified in [RFC4301], that provides IPsec security to tunneled IP packets. IPsec processing is performed by the tunnel endpoints, which can be (but are typically not) the end hosts.

Two-Phase Commit: An agreement protocol that is used to resolve the outcome of an atomic transaction in response to a commit request from the root application. Phase One and Phase Two are the distinct phases of the Two-Phase Commit Protocol.

22 U

UCHAR: A single, unsigned byte.

ULONG: A single, unsigned long integer consisting of 32 bits. This data type can have a range from 0 to 4,294,967,395 (0xffffffff).

Unallocated Disk: A disk that is visible to the local machine but is not formatted with a recognized partitioning format such as MBR or GPT.

UncPath: The location of a file in a network of computers, as specified in **UNC** syntax.

Unicode: The universal character encoding scheme for written characters and text based on the original Unicode Standard, Version 2.0 beta (as specified in [UNICODE]). Windows has maintained compatibility with later versions of the Unicode Standard. The Unicode Standard defines a consistent way of encoding multilingual text. The Unicode Standard provides three encoding forms:

A default 16-bit, fixed-width form called UTF-16,

A byte-oriented, variable-width form called UTF-8

A 32-bit form called UTF-32

In this specification, all references to Unicode refer to a single Unicode character or an array of Unicode characters using the 16-bit UTF-16 form of the encoding. In this specification, when arrays of Unicode characters are defined, details are included that indicate if the array of Unicode characters is null-terminated.

The Unicode version used by Windows varies by release but is not changed by service packs. Subsequent versions of Unicode are supersets of the previous versions. The versions are:

Windows Version	Unicode Version	Notes
Windows NT 4.0	Unicode 2.0 beta [UNICODE20]	Essentially Unicode 1.1 plus some fixes to Unicode. For Unicode releases prior to version 4 see http://www.unicode.org/versions/components-pre4.html
Windows 2000	Unicode 3.0 [UNICODE30]	
Windows XP, Windows Server 2003	Unicode 3.2 [UNICODE32]	Collation rules were amended to Unicode 1.1, and not picked up.
Windows Vista	Unicode 5.0 [UNICODE50]	Windows Vista uses Unicode by default. Some standards may be at a Unicode lower level - such as International Domain Names which standardized on Unicode 3.2. For Unicode version 5 see http://www.unicode.org/versions/enumeratedversions.html

Unicode String: A UTF8 null-terminated string used to encode Unicode characters.

Uniform Resource Locator (URL): A string of characters in a standardized format that identifies a document or resource on the World Wide Web.

Unique Identifier (UID): The Distributed File System Replication Protocol associates a unique identifier as a pair consisting of a GUID and a version sequence number to identify each resource uniquely. This **UID** is used to track the object for its entire lifetime through any number of times that the object is modified or renamed.

Universal Disk Format (UDF): A type of file system for storing files on optical media.

Universal Group: A group that can appear in ACLs anywhere in the forest, and can contain other universal groups, global groups, and users from anywhere within the forest.

Universal Naming Convention (UNC): A standard naming format for specifying the location of network resources such as shared files or devices on a network. The format is "\\<servername>\<share>\<filename>", where <servername> is a NetBIOS name, FQDN domain name, or IPv4 address; <share> is a logical share point for accessing <servername>; and <filename> is the name of the file or device.

Universal Serial Bus (USB): A device connectivity specification.

Universally Unique Identifier (UUID): A 128-bit globally unique value used in cross-process communication to identify entities, such as client and server interfaces, manager entry-point vectors, and RPC objects. For more information, see [C706]. See also Globally Unique Identifier.

Unmarshal: (1) The process of deserializing one or more data structures from an octet stream using a specific transfer syntax. For example, unmarshaling a 32-bit integer.

(2) In RPC, the process of decoding one or more data structures from an octet stream using a specific RPC Transfer Syntax.

Unmasked Disk: A disk that is visible to the local machine.

Unnamed Stream: See Main Stream.

Unplug a Channel: The act of switching a channel from plugged channel mode to unplugged channel mode.

Unplugged Channel Mode: A channel mode in which an IN channel or OUT channel instance sends Protocol Data Units (PDUs) immediately instead of queuing them. This is the default mode for channels.

Update: An add, modify, or delete of one or more objects or attribute values.

UPDATE: The set of metadata that pertains to a file, or a file deletion. The main fields in an update consist of the **UID**, **GVSN**, File name, file attributes and flags indicating whether the update is for an existing file, or whether it is for a file deletion.

Update Sequence Number (USN): (1) A monotonically increasing sequence number used in assigning a stamp to an originating update. For more information, see [MS-ADTS].

(2) The offset from the beginning of the change journal stream that uniquely identifies a change journal record.

(3) Contains a 64-bit value representing the number of 100-nanosecond intervals since January 1, 1601 (UTC). This is updated whenever the packageRegistration object is modified on the server to match the server's UTC time at the time of the update.

Updates: A set of UPDATE entities.

Upgrade: A relationship between software packages in which the upgrading application will replace a particular software installation package, the upgraded application, if it exists on a client and was installed through the software installation protocol extension. Logically, this means the client application will be uninstalled and the upgrading application will be installed.

Upgrading Application: If two applications are related due to an upgrade, this is the application to remove from the client when the upgrading application is installed.

Uplevel Trust: A trust in which both peers are running Windows 2000 or later domain controllers.

Upstream Partner: The partner that sends out change orders, files, and folders.

URI: This term is used as specified in [RFC2616].

URL: See **Uniform Resource Locator (URL)**.

User Account Control (UAC): A set of security options associated with a security principal. Particular options designate the role computers in the domain.

User Account Database: A database that maintains user account information.

User Account Database Replication: A mechanism for synchronizing the user accounts database among multiple domain controllers.

User Agent: An HTTP user agent, as specified in [RFC2616].

User Assistance Resource: A UnicodeString containing a URL pointing to information that may be helpful to users of the application when viewing information about the application through a software maintenance tool. This is defined by the administrator who deploys the application.

User Connection: A connection to a printer (shared from a print server) on a client machine. A connection is displayed in the user interface as a printer. User connections are displayed for only one user of a particular client machine.

User Datagram Protocol (UDP): The connectionless protocol within TCP/IP that corresponds to the transport layer in the ISO/OSI reference model.

User-Defined Message Tag (MTAG): A message that is sent within the context of an established connection. See also Message Tag (MTAG).

User GPO Version: A version number of the changes for the user policy portion of a Group Policy object (GPO). This is a 16-bit integer encoded in the upper 16 bits of a GPO version.

User Message: A message sent between instances of an application using the DirectPlay network library as a transport.

User Object: An object of class **user**. A user object is a security principal object; the principal is a person or service entity running on the computer. The shared secret allows the person or service entity to authenticate itself.

User Policy Mode: A mode of policy application used to retrieve settings for an authenticated domain user account, interactively logged on to a client.

User Principal Name (UPN): A user account name (sometimes referred to as the user logon name) and a domain name identifying the domain in which the user account is located. This is the standard usage for logging on to a Windows domain. The format is:

someone@example.com (in the form of an e-mail address). In Active Directory, the userPrincipalName attribute of the account object, as specified in [MS-ADTS].

User Profile: A collection of attributes on a user object that are used to customize an end-user experience.

User Profile Folder: A storage location in an operating system that provides the operating system and applications with a per-user location with conventional semantics. For example, each user on a Windows operating system has his or her own documents, music, videos, and pictures user-profile folders in which they may store per-user data.

User-Scoped Group Policy Object (GPO) Distinguished Name (DN): A scoped Group Policy object (GPO) distinguished name (DN) that begins with "CN=User."

User-Scoped Group Policy Object (GPO) Path: A scoped Group Policy object (GPO) path that ends in "\User."

USHORT: A single, unsigned short integer consisting of 16 bits. This data type can have a range from 0 to 65,535 (0xffff).

USN: See **Update Sequence Number**.

UTC (Coordinated Universal Time): A high-precision atomic time standard that approximately tracks Universal Time (UT). It is the basis for legal, civil time all over the Earth. Time zones around the world are expressed as positive and negative offsets from UTC. In this role, it is also referred to as Zulu time (Z) and Greenwich Mean Time (GMT). In these specifications, all references to UTC refer to the time at UTC–0 (or GMT).

UTF-16: A standard for encoding Unicode characters, defined in the Unicode standard, in which the most commonly used characters are defined as double-byte characters.

UTF-16LE (Unicode Transformation Format, 16-bits, Little-Endian): The encoding scheme specified in [UTF16] for encoding Unicode (see [Unicode30]) characters as a sequence of 16-bit codes, each encoded as two 8-bit bytes with least-significant-byte first.

UTF-8: A byte-oriented standard for encoding Unicode characters, defined in the Unicode standard.

UUID: See **Universally Unique Identifier**.

UUID or GUID: See **Universally Unique Identifier**. See Globally Unique Identifier (GUID).

23 V

Value: A data element associated with a key.

Virtual Disk Service (VDS) Object: An instance of a class that exposes one or more DCOM interfaces to query or configure the **Virtual Disk Service**, the operating system device (such as a disk or volume), or the concept (such as a software provider), that the object represents.

Virtual Disk Service (VDS) Provider: A concept that models the software responsible for storage management. A VDS software provider performs operations on disk and volume devices exposed to the operating system.

Virtual Disk Service (VDS) Session: The point at which a client receives an instance of the VDS service object to the point at which it releases it. Unless otherwise indicated, the term **session** refers to a VDS session.

Vendor ID Payload: A particular type of **ISAKMP payload** that contains a vendor-defined constant. The constant is used by vendors to identify and recognize remote instances of their implementations. This mechanism allows a vendor to experiment with new features while maintaining backward compatibility. For more information, see [RFC2408] section 3.16.

Version Chain Vector: A data structure that maps machine GUIDs to sets of version sequence numbers.

Version Sequence Number (VSN): A 64-bit unsigned number. **Version sequence numbers** are assigned to global version sequence numbers as part of file metadata in monotonic increasing order.

Global Version Sequence Numbers (GVSN): A number that consists of a machine identifier (which is a GUID) and a **version sequence number**. A **GVSN** is used to identify a unique version of a unique resource. In other words, no two different resources ever get assigned the same **GVSN**, and no two different updates to the same resource ever get assigned the same **GVSN**.

Version Vector: (1) A mapping from machine identifiers to **version sequence numbers**. Distributed File System Replication Protocol uses a generalization of version vectors called **version chain vectors**.

(2) A vector of **volume sequence numbers (VSNs)**, with one entry per replica set member, as identified by originator GUID. All change orders carry the originator GUID of the originating member and the associated **VSN**. As each replica member receives the update, it tracks the **VSN** in a vector slot that is assigned to the originating member. This vector specifies whether the replica tree is current with each member. The version vector is then used to filter updates from inbound partners that may have already been applied. The version vector is also delivered to the inbound partner when the two members join. When a new connection is created, the version vector is used to scan the file ID table for more recent updates that are not seen by the new outbound partner.

Version Vector Join (vvjoin): The process in which a downstream partner joins with an upstream partner for the first time. It is also called initial sync.

Virtual Cluster Number (VCN): The cluster number relative to the beginning of the file, directory, or stream within a file.

Virtual Connection: (1) A pair consisting of one virtual IN channel and one virtual OUT channel between the same RPC client and RPC server that provides full-duplex, reliable, in-order, at-most-once delivery communication capabilities.

(2) An SMB Connection between an SMB client and SMB server.

Virtual Disk Service (VDS): The service component running on the server.

Virtual IN Channel: A communication session between an remote procedure call (RPC) client and an remote procedure call (RPC) server that can span multiple IN channels. When the communication session spans multiple IN channels, the IN channels are sequentially ordered in time with partial overlap in time between channel N and channel N+1 in the sequence. A virtual IN channel provides half-duplex, RPC client-to-RPC server, reliable, in-order, at-most-once delivery communication capabilities.

Virtual OUT Channel: A communication session between an remote procedure call (RPC) client and an remote procedure call (RPC) server that can span multiple OUT channels. When the communication session spans multiple OUT channels, the OUT channels are sequentially ordered in time with partial overlap in time between channel N and channel N+1 in the sequence. A virtual OUT channel provides half-duplex, RPC server-to-RPC client, reliable, in-order, at-most-once delivery communication capabilities.

Volume: A group of one or more partitions that forms a logical region of storage and the basis for a file system. A **volume** is an area on a storage device that is managed by the file system as a discrete logical storage unit. A partition contains at least one **volume**, and a volume can exist on one or more partitions.

Volume Data: Data stored on a **volume**.

Volume Identifier (VolumeId): A 128-bit value used to represent a **volume**. The value of a **VolumeId** is unique on a single computer (the local file system or a remote file server).

Volume Label: See **File System Label**.

Volume Manager: A system component that manages communication and data transfer between applications and disks.

Volume Members: See RAID Column.

Volume Mount Name: A path for a volume. The path consists of a GUID formatted as a string. Applications can use this path to open the volume.

Volume Parity (SCSI): See RAID Column. See **RAID-5**.

Volume Plex: A member of a **volume** that represents a complete copy of data stored. For instance, mirrored volumes have more than one plex.

Volume Sequence Number (VSN) (for File Replication Service): A unique sequence number assigned to a change order to order the event sequence in a replica. It is a monotonically increasing sequence number assigned to each change that originates on a given replica member. If one change order has a smaller **volume sequence number (VSN)** than another change order, the change the first change order represents occurs before the change that the second change order represents.

VolumeID: A unique identifier that represents the identity of a file system volume.

VolumeInformation: Information about a volume, which is stored on the volume, such as its VolumeID and VolumeSequenceNumber.

VolumeOwner: A MachineID that is considered to be the owner of a VolumeID. A VolumeID can only have one VolumeOwner. For more information, see [MS-DLTM].

VolumeSecret: A value that is used to establish a VolumeOwner. For more information, see [MS-DLTM].

VolumeSequenceNumber: An integer value used to track the sequence of move notification messages received by the protocol server.

VolumeTable: Maps a VolumeID to a RefreshTime, VolumeSequenceNumber, VolumeSecret, and VolumeOwner. For more information, see [MS-DLTM].

vvjoin: See **Version Vector Join (vvjoin)**.

24 W

Well-Known Endpoint: A preassigned, network-specific, stable address for a particular client/server instance. For more information, see [C706].

Well-Known Security Identifier (SID): One of a number of security identifiers (SIDs) that has a constant value.

Window Menu: A context menu associated with a window or notification icon that contains a list of common operations to perform such as minimize, maximize, move, and so on.

Windows-1252: See **ANSI Character Set**.

Window Coordinates: Coordinates relative to the top-left corner of the window.

Window Visible Region: The portion of the window that is not obscured by other user interface elements.

Windows Error Code: A 32-bit quantity where zero represents success and non-zero represents failure. The specific failure codes are specified in [MS-ERREF].

Windows Metafile Format (WMF): A file format used by Windows that supports the definition of images.

Windows NT Account Name: A string identifying the name of a Windows NT account.

Windows NT Domain: A domain hosted entirely on Windows NT 4.0 servers.

Windows NT Domain Name: A string identifying the name of a Windows NT domain to which an identity belongs.

Windows NT Password: A string of 0 to 256 case-sensitive Unicode (as specified in [RFC2781]) characters used to prove entitlement to a Windows NT account.

Windows Registry: The Windows implementation of the registry.

Windows Security Descriptor: A Windows NT security descriptor.

Windows Server Enterprise: A version (also referred to as a Stock Keeping Unit (SKU) of the Windows Server 2003 R2 operating system.

Windows Time Service (W32Time): A time service implemented on Windows 2000 and later releases. The service supports time synchronization against network and hardware time sources. For more information, see [WTSREF] and [MS-SNTP].

Windows Internet Name Service (WINS): A name service for the NetBIOS protocol, particularly designed to ease transition to a TCP/IP based network.

Wireless Local Area Network (WLAN): A Local Area Network to which mobile users (clients) can connect and communicate by means of high-frequency radio waves rather than wires. WLANs are specified in the IEEE 802.11 standard [IEEE802.11].

WMI Asynchronous Operation: Defines an operation that is executed on the server side while the client does not wait or query for the results. Instead, the server callbacks the client to communicate the result of the operation.

Wi-Fi Protected Access (WPA): For more information, see [WPA].

Wi-Fi Protected Access 2 (WPA2): For more information, see [WPA2].

WMI Query Language (WQL): A subset of American National Standards Institute Structured Query Language (ANSI SQL). It differs from the standard SQL in that it retrieves from classes rather than tables and returns CIM classes or instances rather than rows.

Writable Naming Context (NC) Replica: A naming context (NC) replica that accepts originating updates. Partial replicas are not writable.

Writability: The abstract feature capability representing the ability of a domain controller (DC) to accept modifications and issue originating updates, with respect to a given naming context (NC) replica.

Write-Protect: An attribute of storage media denoting that the media is not available to be written.

25 X

X.509: An ITU-T standard for Public Key Infrastructure subsequently adapted by the IETF, as specified in [RFC3280].

XA Protocol: The protocol specified in [XOPEN-DTP].

XA Resource Manager Bridge: A software component that allows an application to enlist an XA Resource Manager in an OleTx Transaction.

XA Resource Manager Bridge Facet: A software component that allows a Transaction Manager to communicate with an **XA Resource Manager Bridge**.

XML: The Extensible Markup Language, as specified in [XML1.0].

XP Native Mode: When a user in the Administrator's group logs onto a client computer, the token created is a full token.

26 Z

Z-Order

The top-to-bottom order of the windows on a desktop. Windows lower in the Z-order are obscured by overlapping windows higher in the Z-order.