

1.1 Glossary

Article 09/20/2022

This document uses the following terms:

Active Directory: The Windows implementation of a general-purpose [directory service](#), which uses [LDAP](#) as its primary access protocol. [Active Directory](#) stores information about a variety of objects in the network such as user accounts, computer accounts, groups, and all related credential information used by Kerberos [\[MS-KILE\]](#). [Active Directory](#) is either deployed as Active Directory Domain Services (AD DS) or Active Directory Lightweight Directory Services (AD LDS), which are both described in [\[MS-ADOD\]: Active Directory Protocols Overview](#).

Advanced Encryption Standard (AES): A block cipher that supersedes the Data Encryption Standard (DES). AES can be used to protect electronic data. The AES algorithm can be used to encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. AES is used in symmetric-key cryptography, meaning that the same key is used for the encryption and decryption operations. It is also a block cipher, meaning that it operates on fixed-size blocks of plaintext and ciphertext, and requires the size of the plaintext as well as the ciphertext to be an exact multiple of this block size. AES is also known as the Rijndael symmetric encryption algorithm [\[FIPS197\]](#).

alias: A group that is local to a particular machine (as opposed to a [group](#) that has security permissions and settings for the entire [domain](#)).

authentication: The ability of one entity to determine the identity of another entity by proving an identity to a [server](#) while providing key material that binds the identity to subsequent communications.

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 [\[MS-RPCE\]](#).

authenticator: When used in reference to the Netlogon Protocol, the data stored in the NETLOGON_AUTHENTICATOR structure.

authoritative response: An authoritative response is one in which the server has all necessary resources to service the caller's request. If some of the resources are temporarily unavailable, then the server will indicate that its response is not authoritative. When a server does not return an authoritative response, it is reasonable for the caller to retry the request at another server. The reasons why a request is non-authoritative are always implementation-specific and could include any failure of the server to allocate necessary resources.

backup domain controller (BDC): A [domain controller \(DC\)](#) that receives a copy of the [domain](#) directory database from the [primary domain controller \(PDC\)](#). This copy is synchronized periodically and automatically with the [primary domain controller \(PDC\)](#). BDCs also authenticate user logons and can be promoted to function as the [PDC](#). There is only one [PDC](#) or [PDC](#) emulator in a [domain](#), and the rest are [backup domain controllers](#).

binary large object (BLOB): A collection of binary data stored as a single entity in a database.

binding handle: A data structure that represents the logical connection between a client and a server.

checked build: A special build of an operating system that contains fewer compiler optimizations and more debugging checks than a production environment build. The purpose of the checked build is to make identifying and diagnosing operating system-level problems easier. For more information, see [\[MSDN-CHKBLD\]](#).

client challenge: A 64-bit [nonce](#) generated on the client side.

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. See [security principal](#).

credential: Previously established, authentication data that is used by a security principal to establish its own identity. When used in reference to the Netlogon Protocol, it is the data that is stored in the NETLOGON_CREDENTIAL structure.

database: 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, has to expose a mechanism to enable Netlogon to gather changes from and apply changes to the database. Additionally, it has to export a database serial number in order to track changes for efficient replication.

database serial number: A numeric value that is incremented each time a database transaction is applied to the database.

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

delta: One of a set of possible changes that can be made to a [database](#).

direct trust: A type of authentication functionality in which one [domain](#) accepts another [domain](#) as an authoritative source to provide object authentication and other [Active Directory](#) services for that other [domain](#). For example, if a [direct trust](#) is established from [domain](#), DOMAIN-A, to [domain](#), DOMAIN-B, DOMAIN-A trusts DOMAIN-B. If a [domain](#), DOMAIN-A, has to authenticate an object, such as a user account, from a [domain](#), DOMAIN-B, DOMAIN-A requests that DOMAIN-B authenticate the user account, and DOMAIN-A will treat the response from DOMAIN-B as reliable.

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. See also [Active Directory](#).

DNS name: A [fully qualified domain name \(FQDN\)](#).

domain: A set of users and computers sharing a common namespace and management infrastructure. At least one computer member of the set has to act as a [domain controller \(DC\)](#) and host a member list that identifies all members of the domain, as well as optionally hosting the [Active Directory](#) service. The domain controller provides authentication of members, creating a unit of trust for its members. Each domain has an identifier that is shared among its members. For more information, see [\[MS-AUTHSOD\]](#) section 1.1.1.5 and [\[MS-ADTS\]](#).

domain account: A stored set of attributes representing a principal used to authenticate a user or machine to an [Active Directory](#) domain.

domain controller (DC): The service, running on a server, that implements [Active Directory](#), or the server hosting this service. The service hosts the data store for objects and interoperates with other [DCs](#) to ensure that a local change to an object replicates correctly across all [DCs](#). When [Active Directory](#) is operating as Active Directory Domain Services (AD DS), the [DC](#) contains full NC replicas of the configuration naming context (config NC), schema naming context (schema NC), and one of the domain NCs in its [forest](#). If the AD DS [DC](#) is a global catalog server (GC server), it contains partial NC replicas of the remaining domain NCs in its [forest](#). For more information, see [\[MS-AUTHSOD\]](#) section 1.1.1.5.2 and [\[MS-ADTS\]](#). When [Active Directory](#) is operating as Active Directory Lightweight Directory Services (AD LDS), several AD LDS [DCs](#) can run on one server. When [Active Directory](#) is operating as AD DS, only one AD DS [DC](#) can run on one server. However, several AD LDS [DCs](#) can coexist with one AD DS [DC](#) on one server. The AD LDS [DC](#) contains full NC replicas of the config NC and the schema NC in its [forest](#). The domain controller is the server side of Authentication Protocol Domain Support [\[MS-APDS\]](#).

domain local group: An [Active Directory](#) group that allows user objects, global groups, and universal groups from any [domain](#) as members. It can additionally include, and be a member of, other [domain local groups](#) from within its [domain](#). A group object g is a [domain local group](#) if and only if GROUP_TYPE_RESOURCE_GROUP is present in g!groupType; see [\[MS-ADTS\]](#) section 2.2.12, "Group Type Flags". A security-enabled [domain local group](#) is valid for inclusion within access control lists (ACLs) from its own [domain](#). If a [domain](#) is in [mixed mode](#), then a security-enabled [domain local group](#) in that [domain](#) allows only user objects as members.

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

domain name: A domain name or a [NetBIOS name](#) that identifies a [domain](#).

Domain Name System (DNS): A hierarchical, distributed database that contains mappings of domain names to various types of data, such as IP addresses. DNS enables the location of computers and services by user-friendly names, and it also enables the discovery of other information stored in the database.

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.

dynamic endpoint: A network-specific server address that is requested and assigned at run time. For more information, see [\[C706\]](#).

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.

endpoint: A network-specific address of a remote procedure call (RPC) server process for remote procedure calls. The actual name and type of the endpoint depends on the [RPC](#) protocol sequence that is 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 (RPC Protocol Sequence ncacn_np), an endpoint might be the name of a named pipe. For more information, see [\[C706\]](#).

enterprise network: The network of computer systems in an organization, such as a corporation. An enterprise can span geographical locations and often includes a variety of computer types, operating systems, protocols, and network architectures.

forest: One or more [domains](#) that share a common schema and trust each other transitively. An organization can have multiple [forests](#). A [forest](#) establishes the security and administrative boundary for all the objects that reside within the [domains](#) that belong to the [forest](#). In contrast, a [domain](#) establishes 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](#).

forest trust: A type of [trust](#) where the trusted party is a [forest](#), which means that all [domains](#) in that [forest](#) are trusted.

forest trust information: Information about namespaces, [domain names](#), and [security identifiers \(SIDs\)](#) owned by a trusted [forest](#).

full database synchronization: A mechanism for synchronizing an entire database record set on a particular replication partner.

fully qualified domain name (FQDN): In [Active Directory](#), a fully qualified domain name (FQDN) that identifies a [domain](#).

global catalog (GC): A unified partial view of multiple [naming contexts \(NCs\)](#) in a distributed partitioned directory. The [Active Directory](#) directory service [GC](#) is implemented by GC servers. The definition of [global catalog](#) is specified in [MS-ADTS] section 3.1.1.1.8.

globally unique identifier (GUID): A term used interchangeably with [universally unique identifier \(UUID\)](#) in Microsoft protocol technical documents (TDs). Interchanging the usage of these terms does not imply or require a specific algorithm or mechanism to generate the value. Specifically, the use of this term does not imply or require that the algorithms described in [\[RFC4122\]](#) or [C706] must be used for generating the [GUID](#). See also [universally unique identifier \(UUID\)](#).

group: A collection of objects that can be treated as a whole.

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.

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 Definition Language (IDL): The International Standards Organization (ISO) standard language for specifying the interface for remote procedure calls. For more information, see [C706] section 4.

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 has to have access to an account database for the realm that it serves. [KDCs](#) are integrated into the [domain controller](#) role. It is a network service that supplies tickets to clients for use in authenticating to services.

key list request: A Kerberos protocol message used to request a list of key types the KDC can supply to the client to support single sign-on capabilities in legacy protocols.

Lightweight Directory Access Protocol (LDAP): The primary access protocol for [Active Directory](#). Lightweight Directory Access Protocol (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 \(DS\)](#), as described in [MS-ADTS]. The Lightweight Directory Access Protocol can be either version 2 [\[RFC1777\]](#) or version 3 [\[RFC3377\]](#).

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.

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

mixed mode: A state of an [Active Directory domain](#) that supports [domain controllers \(DCs\)](#) running Windows NT Server 4.0 operating system. Mixed mode does not allow organizations to take advantage of new [Active Directory](#) features such as universal groups, nested group membership, and interdomain group membership. See also native mode.

naming context (NC): An [NC](#) is a set of objects organized as a tree. It is referenced by a Distinguished Name (DN). The DN of the [NC](#) is the distinguishedName attribute of the tree root. The [GUID](#) of the Distinguished Name is the objectGUID attribute of the tree root. The [security identifier \(SID\)](#) of the Distinguished Name, if present, is the objectSid attribute of the tree root; for Active Directory Domain Services (AD DS), the [SID](#) is present if and only if the [NC](#) is a domain naming context (domain NC). [Active Directory](#) supports organizing several [NCs](#) into a tree structure.

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 operating system-compatible network security environment, the component responsible for synchronization and maintenance functions between a [primary domain controller \(PDC\)](#) and backup domain controllers (BDC). [Netlogon](#) is a precursor to the directory replication server (DRS) protocol.

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.

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 extremely small. A nonce is used in authentication protocols to prevent replay attacks. For more information, see [\[RFC2617\]](#).

NT LAN Manager (NTLM): An [authentication](#) protocol that is based on a challenge-response sequence for [authentication](#).

one-way function (OWF): The calculation of a hash of the password using the Rivest-Shamir-Adleman (RSA) MD4 function. [OWF](#) is used to refer to the resulting value of the hash operation.

opnum: An operation number or numeric identifier that is used to identify a specific [remote procedure call \(RPC\)](#) method or a method in an interface. For more information, see [\[C706\]](#) section 12.5.2.12 or [\[MS-RPCE\]](#).

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.

partial database synchronization: A mechanism for synchronizing a set of database records on a particular replication partner.

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 [domain controller \(DC\)](#) designated to track changes made to the accounts of all computers on a [domain](#). It is the only computer to receive these changes directly, and is specialized so as to ensure consistency and to eliminate the potential for conflicting entries in the [Active Directory](#) database. A [domain](#) has only one [PDC](#).

principal: An authenticated entity that initiates a message or channel in a distributed system.

privilege: 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.

RC4: A variable key-length symmetric encryption algorithm. For more information, see [\[SCHNEIER\]](#) section 17.1.

read-only domain controller (RODC): A [domain controller \(DC\)](#) that does not accept originating updates. Additionally, an [RODC](#) does not perform outbound replication. An [RODC](#) cannot be the primary domain controller (PDC) for its domain.

relative identifier (RID): The last item in the series of SubAuthority values in a [security identifier \(SID\)](#) [\[SIDD\]](#). 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 RID.

remote procedure call (RPC): A communication protocol used primarily between client and server. The term has three definitions that are often used interchangeably: a runtime environment providing for communication facilities between computers (the RPC runtime); a set of request-and-response message exchanges between computers (the RPC exchange); and the single message from an RPC exchange (the RPC message). For more information, see [\[C706\]](#).

RPC protocol sequence: A character string that represents a valid combination of a [remote procedure call \(RPC\)](#) protocol, a network layer protocol, and a transport layer protocol, as described in [\[C706\]](#) and [\[MS-RPCE\]](#).

RPC transport: The underlying network services used by the remote procedure call (RPC) runtime for communications between network nodes. For more information, see [\[C706\]](#) section 2.

secret key: A symmetric encryption key shared by two entities, such as between a user and the [domain controller \(DC\)](#), 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.

secure channel: An authenticated [remote procedure call \(RPC\)](#) connection between two machines in a [domain](#) with an established [security context](#) used for signing and encrypting [RPC](#) packets.

Security Account Manager (SAM): A centrally managed service, such as Active Directory Domain Services (AD DS), that enables a server to establish a trust relationship with other authorized servers. The SAM also maintains information about domains and security principals, and provides client-to-server information by using several available standards for access control lists (ACLs).

security account manager (SAM) built-in database: The part of the user account database that contains account information (such as account names and passwords) for accounts and groups that are pre-created at the database installation.

security context: An abstract data structure that contains authorization information for a particular [security principal](#) in the form of a Token/Authorization Context (see [\[MS-DTYP\]](#) section 2.5.2). A server uses the authorization information in a [security context](#) to check access to requested resources. A [security context](#) also contains a key identifier that associates mutually established cryptographic keys, along with other information needed to perform secure communication with another security principal.

Security Descriptor Definition Language (SDDL): The format used to specify a security descriptor as a text string, specified in [\[MS-DTYP\]](#) section 2.5.1.

security identifier (SID): An identifier for [security principals](#) that is used to identify an account or a group. 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 [relative identifier \(RID\)](#). The [SID](#) format is specified in [MS-DTYP] section 2.4.2; a string representation of [SIDs](#) is specified in [MS-DTYP] section 2.4.2 and [MS-AZOD] section 1.1.1.2.

security principal: A unique entity, also referred to as a principal, that can be authenticated by [Active Directory](#). It frequently corresponds to a human user, but also can be a service that offers a resource to other security principals. Other security principals might be a group, which is a set of principals. Groups are supported by [Active Directory](#).

security provider: A pluggable security module that is specified by the protocol layer above the [remote procedure call \(RPC\)](#) layer, and will cause the [RPC](#) layer to use this module to secure messages in a communication session with the server. The security provider is 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 [Security Support Provider Interface \(SSPI\)](#) 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 NTLM.

Security Support Provider Interface (SSPI): An API that allows connected applications to call one of several security providers to establish authenticated connections and to exchange data securely over those connections. It is equivalent to Generic Security Services (GSS)-API, and the two are on-the-wire compatible.

server: A computer on which the [remote procedure call \(RPC\)](#) server is executing.

server challenge (SC): A 64-bit nonce generated on the server side.

service principal name (SPN): The name a client uses to identify a service for mutual authentication. For more information, see [MS-ADTS] section 2.2.21 (Service Principal Name) and [RFC1964] section 2.1.1.

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](#) has to be strong enough to withstand cryptanalysis for the lifespan of the session.

shared secret: A piece of data that is known only to the [security principal](#) and an authenticating authority; for example, a user and a domain controller. It is used to prove the [principal's](#) identity. A password is a common example of a shared secret. Also called a "secret key".

site: A collection of one or more well-connected (reliable and fast) TCP/IP subnets. By defining [sites](#) (represented by site objects) an administrator can optimize both [Active Directory](#) access and Active Directory replication with respect to the physical network. When users log in, Active Directory clients find [domain controllers \(DCs\)](#) that are in the same site as the user, or near the same site if there is no [DC](#) in the site. See also Knowledge Consistency Checker (KCC). For more information, see [MS-ADTS].

sub-authentication: Optional and additional [authentication](#) functionality, usually provided by extending an [authentication](#) algorithm.

sub-authentication package: An optional component that provides additional [authentication](#) functionality. If a [sub-authentication package](#) is installed, the [authentication](#) package calls the [sub-authentication package](#) before returning its [authentication](#) result. The request to verify by a [sub-authentication package](#) is indicated by the ParameterControl field of the LogonInformation parameter (see [MS-APDS] section 3.1.5.2.1, Verifying Responses with Sub-Authentication Packages).

Time-To-Live (TTL): The time duration for which a Server Object is available.

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 can be configured to trust domain C through transitive trust.

trust: To accept another authority's statements for the purposes of [authentication](#) and authorization, especially in the case of a relationship between two domains. If [domain A](#) trusts [domain B](#), [domain A](#) accepts [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 between two [domains](#) described in the previous sentence.

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 that define a trust relationship with another domain, such as direction (outbound, inbound, or both), trust attributes, name, and security identifier of the other domain. For more information, see [MS-ADTS].

Unicode: A character encoding standard developed by the Unicode Consortium that represents almost all of the written languages of the world. The [Unicode](#) standard [UNICODE5.0.0/2007] provides three forms (UTF-8, UTF-16, and UTF-32) and seven schemes (UTF-8, UTF-16, UTF-16 BE, UTF-16 LE, UTF-32, UTF-32 LE, and UTF-32 BE).

Unicode string: A [Unicode](#) 8-bit string is an ordered sequence of 8-bit units, a [Unicode](#) 16-bit string is an ordered sequence of 16-bit code units, and a [Unicode](#) 32-bit string is an ordered sequence of 32-bit code units. In some cases, it could be acceptable not to terminate with a terminating null character. Unless otherwise specified, all [Unicode strings](#) follow the UTF-16LE encoding scheme with no Byte Order Mark (BOM).

universally unique identifier (UUID): A 128-bit value. UUIDs can be used for multiple purposes, from tagging objects with an extremely short lifetime, to reliably identifying very persistent objects in cross-process communication such as client and server interfaces, manager entry-point vectors, and [RPC](#) objects. UUIDs are highly likely to be unique. UUIDs are also known as [globally unique identifiers \(GUIDs\)](#) and these terms are used interchangeably in the Microsoft protocol technical documents (TDs). Interchanging the usage of these terms does not imply or require a specific algorithm or mechanism to generate the UUID. Specifically, the use of this term does not imply or require that the algorithms described in [RFC4122] or [C706] must be used for generating the UUID.

user principal name (UPN): A user account name (sometimes referred to as the user logon name) and a domain name that identifies 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 email address). In [Active Directory](#), the userPrincipalName attribute of the account object, as described in [MS-ADTS].

Windows Time Service (W32Time): A service that supports time synchronization against network and hardware time sources. For more information, see [\[WTSREF\]](#) and [\[MS-SNTP\]](#).

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.

writable domain controller: A [domain controller](#) that performs originating updates and outbound replication.

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as defined in [\[RFC2119\]](#). All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.