Keberos Delegation

Kerberos is an authentication protocol that is used to verify the identity of a user or host

The Windows Server operating systems implement the Kerberos version 5 authentication protocol and extensions for public key authentication, transporting authorization data, and delegation. The Kerberos authentication client is implemented as a security support provider (SSP), and it can be accessed through the Security Support Provider Interface (SSPI). Initial user authentication is integrated with the Winlogon single sign-on architecture.

The Kerberos Key Distribution Center (KDC) is integrated with other Windows Server security services that run on the domain controller. The KDC uses the domain's Active Directory Domain Services database as its security account database. Active Directory Domain Services is required for default Kerberos implementations within the domain or forest

Delegated authentication

Services that run on Windows operating systems can impersonate a client computer when accessing resources on the client's behalf. In many cases, a service can complete its work for the client by accessing resources on the local computer. When a client computer authenticates to the service, NTLM and Kerberos protocol provide the authorization information that a service needs to impersonate the client computer locally. However, some distributed applications are designed so that a front-end service must use the client computer's identity when it connects to back-end services on other computers. Kerberos authentication supports a delegation mechanism that enables a service to act on behalf of its client when connecting to other services.

Using Kerberos authentication within a domain or in a forest allows the user or service access to resources permitted by administrators without multiple requests

for credentials. After initial domain sign on through Winlogon, Kerberos manages the credentials throughout the forest whenever access to resources is attempted