SPN Kerberos Delegierung

Was ist denn nun genau ein SPN?

Also, ein Dienstprinzipalname (Service Principal Name) SPN, ist ein eindeutiger Name der eine Instanz eines Service identifiziert und ist verbunden mit dem Login-Konto unter dem die Instanz läuft.

Es stellt eine Zuordnung zwischen dem AD-Account und der Dienstinstanz her. Er besteht aus einem mehrteiligen Namensformat wie z.B. http/webserver.ndsedv.de.

Der SPN wird in den Prozess der gegenseitigen Authentifizierung zwischen einem Client und einem Server eingesetzt der einen bestimmten Dienst verwendet.

Ein SPN kann aber auch an ein Benutzer- (Dienst-) Konto verknüpft werden, wenn ein Dienst oder eine Anwendung unter diesem Benutzer ausgeführt wird.

Das würde dann z.B. so aussehen:
setspn -A HTTP/benutzer1.ndsedv.de@ndsedv.de benutzer1

Eingesetzt werden SPNs ganz stark im SQL-Server Umfeld. Dort läuft der SQL-Server-Dienst in der Regel unter einem Dienstkonto anstatt unter „LocalSystem“.

Das Ganze würde dann z.B. so aussehen: MSSQLSvc/sqlsrvr.ndsedv.de:1433

Um einen Überblick über die SPNs zu bekommen, kann man den Befehl setspn –L einsetzen. Es werden einem alle registrierten SPNs aufgelistet. Der Befehl klist wäre eine Alternative.

Zur Abfrage kann aber auch LDP oder LDIFDE eingesetzt werden.

Server_2012_-_SPN_und_Kerberos_Delegierung