کربروس Kerberos دو نوع نام اصلی Principal Names مختلف را تعیین یا مشخص میکند. این دو نام اصلی مختلف، یکی User Principal Name – UPN است و دیگری Service Principal Name – SPN میباشد.

فقط اکانت یوزر User account دارای یک User Principal Name – UPN است که در اکانت آن یوزر معین یا مشخص شده است. وقتی شما اکانت یک یوزر را نگاه کنید، در تب اکانت Account، متوجه میشوید که UPN از ترکیب دو قسمت Field که در قسمت User logon name قرار دارند تشکیل شده است. یک UPN باید در کل Forest منحصر بفرد unique باشد، در غیر این صورت زمانی که [KDC](https://msdn.microsoft.com/en-us/library/windows/desktop/aa378170(v=vs.85).aspx)به اکانت یوزرها با استفاده از UPN نگاه میکند، اگر چند یوزر دارای یک UPN باشند، احراز هویت Authentication برای تمام آن یوزرها که دارای UPN یکسان هستند با شکست یا عدم موفقیت failures مواجه خواهد شد. UPN در object اکتیو دایرکتوری یک صفت attribute است که فقط میتواند یک مقدار تک یا واحد را در خود داشته باشد. اسم این صفت attribute که این مقدار واحد یا تک را در خود دارد userPrincipalName میباشد. به طور مثال UPN به این صورت است : Administrator@GEEKBOY.IR

Service Principal Names باید در Forest منحصر بفرد باشد و میتواند به اکانت یوزر User account یا اکانت کامپیوتر Computer account اختصاص داده شود. فقط برای اکانت کامپیوتر Computer account است که به صورت اتوماتیک SPN معین یا مشخص میشود.

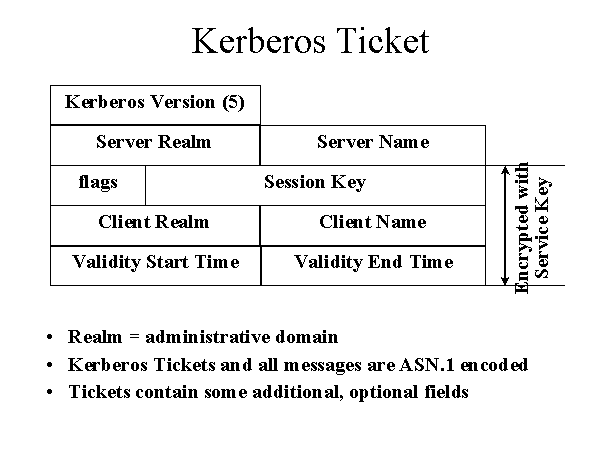
SPN مشخص میکند که کدام سرویس Service در چهار چوب اکانت های امنیتی اجرا شود. بطور مثال برخی از سرویس هایی که یک کامپیوتر میتواند داشته باشد File Server یا CIFS – Common Internet File System میباشد. اگر این کامپیوتر یک دومین کنترولر باشد، یک LDAP SPN و Active Directory Replication SPN و FRS SPN دارد. SPN ها میتوانند برای اکانت یوزر معین یا مشخص شوند که چه زمانی یک سرویس یا برنامه در چهار چوب امنیت یوزرها اجرا شود. بطور معمول این نوع از اکانت های یوزر به نام Service Accounts نامیده میشوند. این خیلی مهم است که بفهمید Service Principal Names باید به صورت منحصر بفرد در Forest اکتیو دایرکتوری باشد.

**در زیر چند نمونه از این اکانت یوزرها که به آنها معین میشود را نگاه میکنیم:**

وقتی یک سرویس سرور SQL بجای استفاده بصورت استاندارد از LocalSystem، از یک اکانت یوزر یا Service Account استفاده میکند. مثال MSSQLSvc/sqlsrvr.geekboy.pro:1433

وقتی یک مخزن برنامه وب Web Application Pool در IIS، در حال اجرا با استفاده از اکانت یک یوزر میباشد، بجای اینکه از Network Service بصورت استداندارد استفاده کند. مثل http/websrvr.geekboy.pro

مجوزها یا بلیط های کربروس Kerberos tickets

[](http://geekboy.pro/wp-content/uploads/2016/07/img007.gif)

**مرکز توزیع کلید Key Distribution Center – KDC**

KDC یک سرویس Service است که فقط و باید بر روی دومین کنترولر Domain Controller در حال کار یا اجرا باشد. اسم این سرویس مرکز توزیع کلید کربروس Kerberos Key Distribution Center است. در واقع KDC یک سرویس است که مسئول تصدیق هویت یوزرها در زمانی که از کربروس استفاده میشود، میباشد. KDC دو جزء component سرور را پیاده سازی میکند. یکی سرور احراز هویت یا تائید Authentication Server – AS است و دیگری سرور اعطای مجوز Ticket Granting Server – TGS میباشد .

**سرور احراز هویت یا تائید Authentication Server – AS**

نقش KDC این است که هویت را شناسایی میکند که principal باشد و سپس درخواست اعطای بلیط یا مجوز Ticket Granting Ticket – TGT را برای اصل بودن principal صادر میکند تا ابراز هویت Authentication با موفقیت انجام شود. داشتن یک TGT معتبر سبب میشود که principal بتواند یک درخواست بلیط یا مجوز سرویس Service ticket از سرور اعطای مجوز Ticket Granting Server – TGS کند. این سبب میشود که یک TGT در کش اعتبار نامهCredentials Cache هر دومین Domain برای principal باشد.