Description:

System.exe:
Kernel mod thread'lerin yürütülmesinden sorumludur. (Drivers)
User: Local System

Svchost.exe:
Generic Host Process for Windows Services. Sayısı az veya çok olabilir. Gruplama mantığında ilerler. Servise bağlı olarak Local System, Network Service, Local Service accountları ile çalıştırılabilir. "-k" ile gruplama yapılır.
Ram Miktarı 3.5GB Üzeri ise gruplama daha azdır.
Instance Sayısı: 10'dan fazla.

Smss.exe:
Server Management SubSystem. Master instance child'ları açar sonra child'laar kendisini kapatır bu sebeple 1 adet running durumda smss görmek normaldir. Session sayısı ile orantılı olarak açılan proocess sayısı artabilir.
Account: Local System

Csrss.exe:
Process ve threadlerin yönetiminden sorumludur. Windows API' deki birçok DLL'in import edilmeside görevlerindendir.
Local System
2 veya daha fazla Instance. (Session Sayısına bağlıdır.)
RDP veya Fast Switch User durumuna göre instance sayısı artabilir.

Services.exe:
Servis ve Tasklar için home process diyebiliriz. Kullanıcı oturum açtığında "HKLM\SYSTEM\Select\LastKnownGood" değerini set eder.
Local System.

Lsaiso.exe:
1 adet-Credential Guard-Local System

Explorer.exe:
Interactive user sayısına göre sayı artabilir.
"HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell" değerinde belirtilir.
Account: Logged On User
Time: İlk process oturum açıldığında oluşur.
System32 altında değildir. "%SYSTEMROOT%" yani "C:\Windows" altındadır.

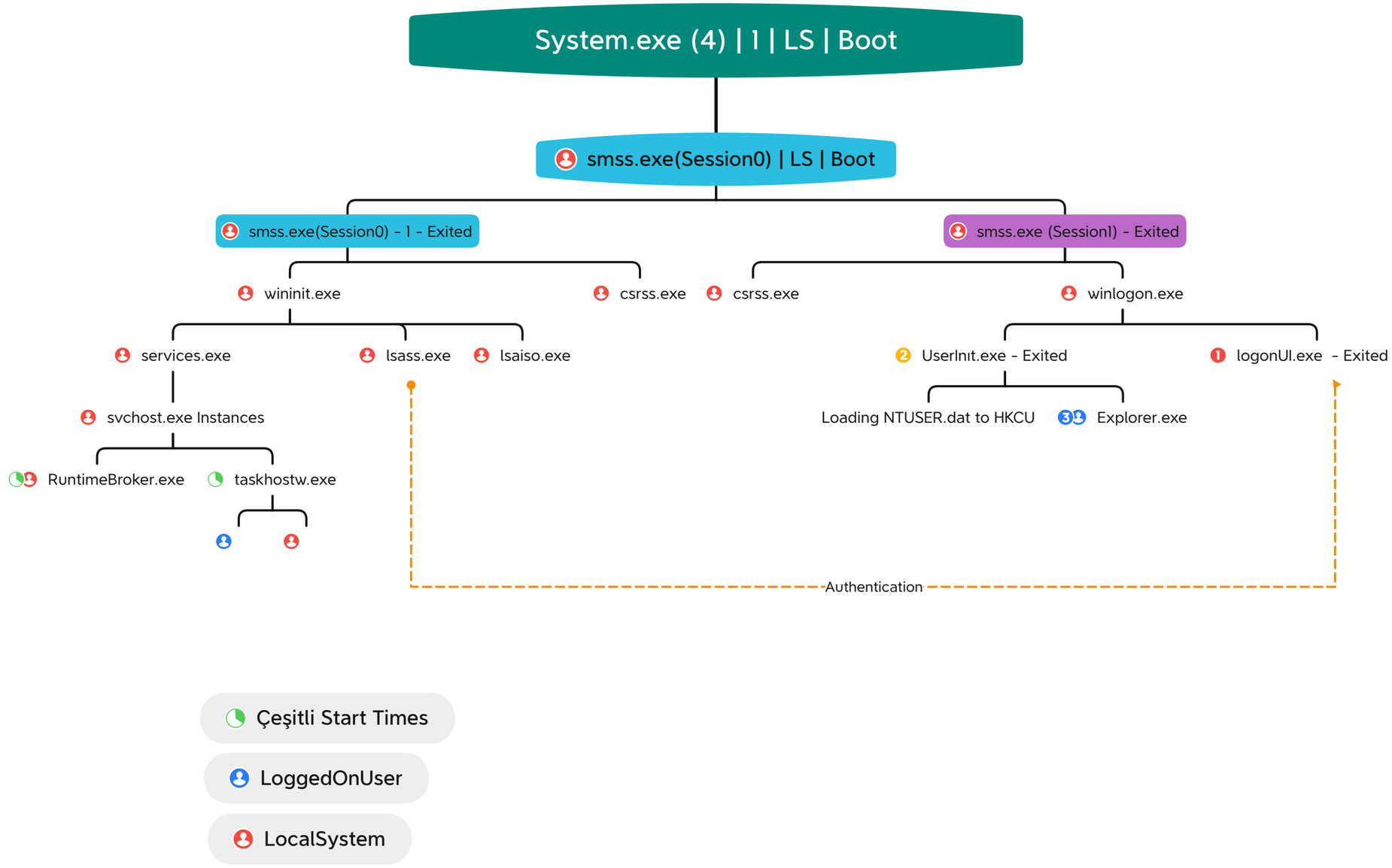
Wininit.exe:
1 Adet bulunur. Local System.

Winlogon.exe:
Local System.
1 veya Daha fazla instance (Oturum açan user'a göre)

Lsass.exe:
Local System.
1 adet.
"HKLM\SYSTEM\CurrentControlSet\Control\Lsa" altındaki değere göre auth işlemi. (Kerberos or MSV1_0).
Security event loglarının yazılması.

Taskhostw.exe:
Local System veya LoggedOnUsers.
1 veya Daha fazla.
Start time çeşitli.
Arka plan tasklarının manage edilmesi.

RuntimeBroker.exe:
1 veya daha fazla..
Local System.
Start time çeşitli.
Metro Apps.



Çeşitli Start Times

LoggedOnUser

LocalSystem