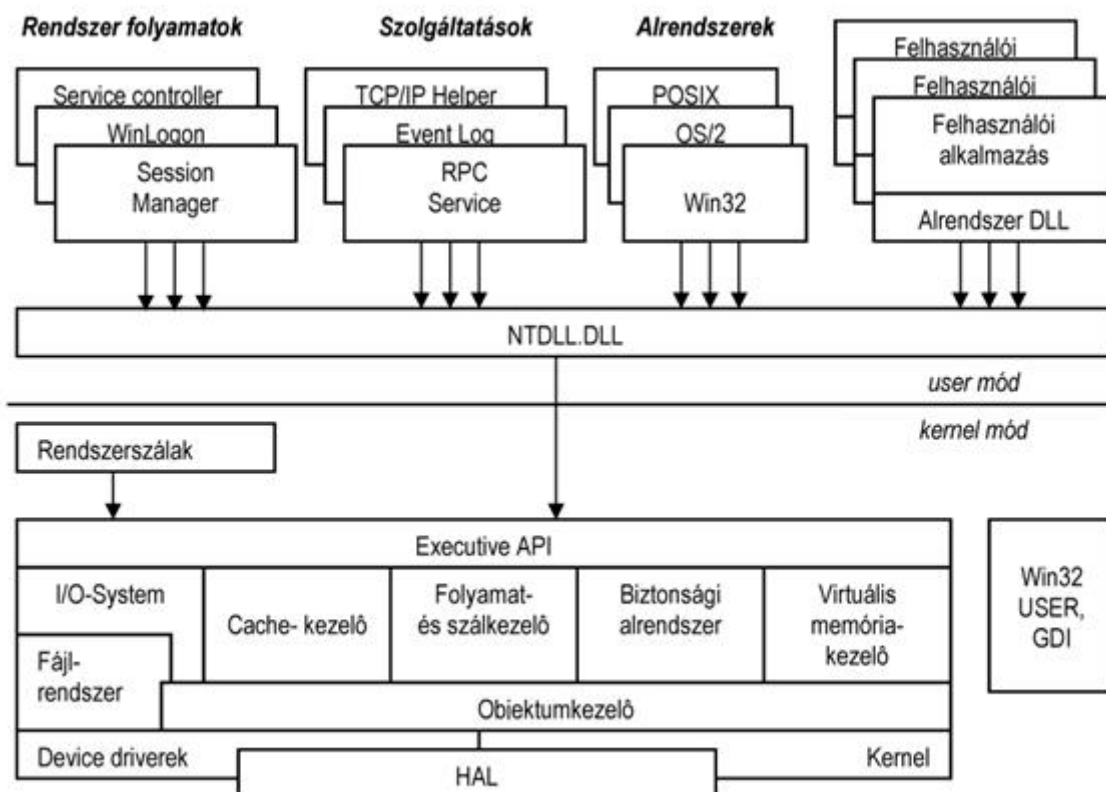


b, kernel32.dll függőségek:

c, NTDLL.DLL

felépítése:



























NTDLL.DLL

Az NTDLL.DLL az a dinamikusan kapcsolódó könyvtár (*Dinamically Linked Library - DLL*), amin keresztül a felhasználói módú folyamatok elérhetik az NT-t. Mivel az egyes objektumok közötti kapcsolattartás az LPC mechanizmuson keresztül történik, így minden felhasználói objektum az NTDLL.DLL-en keresztül éri el a környezetét.

Az NTDLL által megvalósított működés egyszerű. Ha egy hívás érkezik, ellenőrzi a hívás paramétereit, és megvalósítja a *user-kernel* módváltást, majd meghívja az NT kért funkciót megvalósító függvényét.

#### NTDLL.DLL

-  API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
-  API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL
-  API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL
-  } API-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL
-  } API-MS-WIN-ADVAPI32-REGISTRY-L1-1-1.DLL
-  } API-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL
-  } API-MS-WIN-NTUSER-STRING-L1-1-0.DLL
-  } API-MS-WIN-KERNEL32-FILE-L1-1-0.DLL
-  } API-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL
-  } API-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL
-  } API-MS-WIN-KERNEL32-QUIRKS-L1-1-1.DLL
-  } API-MS-WIN-KERNEL32-SIDEBYSIDE-L1-1-0.DLL
-  } API-MS-WIN-MRMCORER-RESMANAGER-L1-1-0.DLL
-  } API-MS-WIN-GPAPI-GROUPPOLICY-L1-1-0.DLL
-  } API-MS-WIN-NTDSAPI-ACTIVEDIRECTORYCLIENT-L1-1-0.DLL
-  } API-MS-WIN-NTDSAPI-ACTIVEDIRECTORYCLIENT-L1-1-1.DLL
-  } API-MS-WIN-SHELL32-SHELLCOM-L1-1-0.DLL
-  } API-MS-WIN-ADVAPI32-NTMARTA-L1-1-0.DLL
-  } API-MS-WIN-SECURITY-CAPAUTHZ-L1-1-1.DLL
-  } API-MS-WIN-FECLIENT-ENCRYPTEDFILE-L1-1-0.DLL
-  } API-MS-WIN-SECURITY-EFSWRT-L1-1-0.DLL
-  } API-MS-WIN-SECURITY-SDDL-L1-1-0.DLL
-  } API-MS-ONECORE-APPMODEL-STATEREPOSITORY-CACHE-L1-1-0.DLL
-  } API-MS-WIN-APPMODEL-DAXCORE-L1-1-0.DLL