HOCHSCHULE MITTWEIDA
University of Applied Sciences

Betriebssysteme
Windows Historie, Kernel

Bundeskriminalamt

Autor: Tim Wetterau

Stand 13.05.2024

Agenda

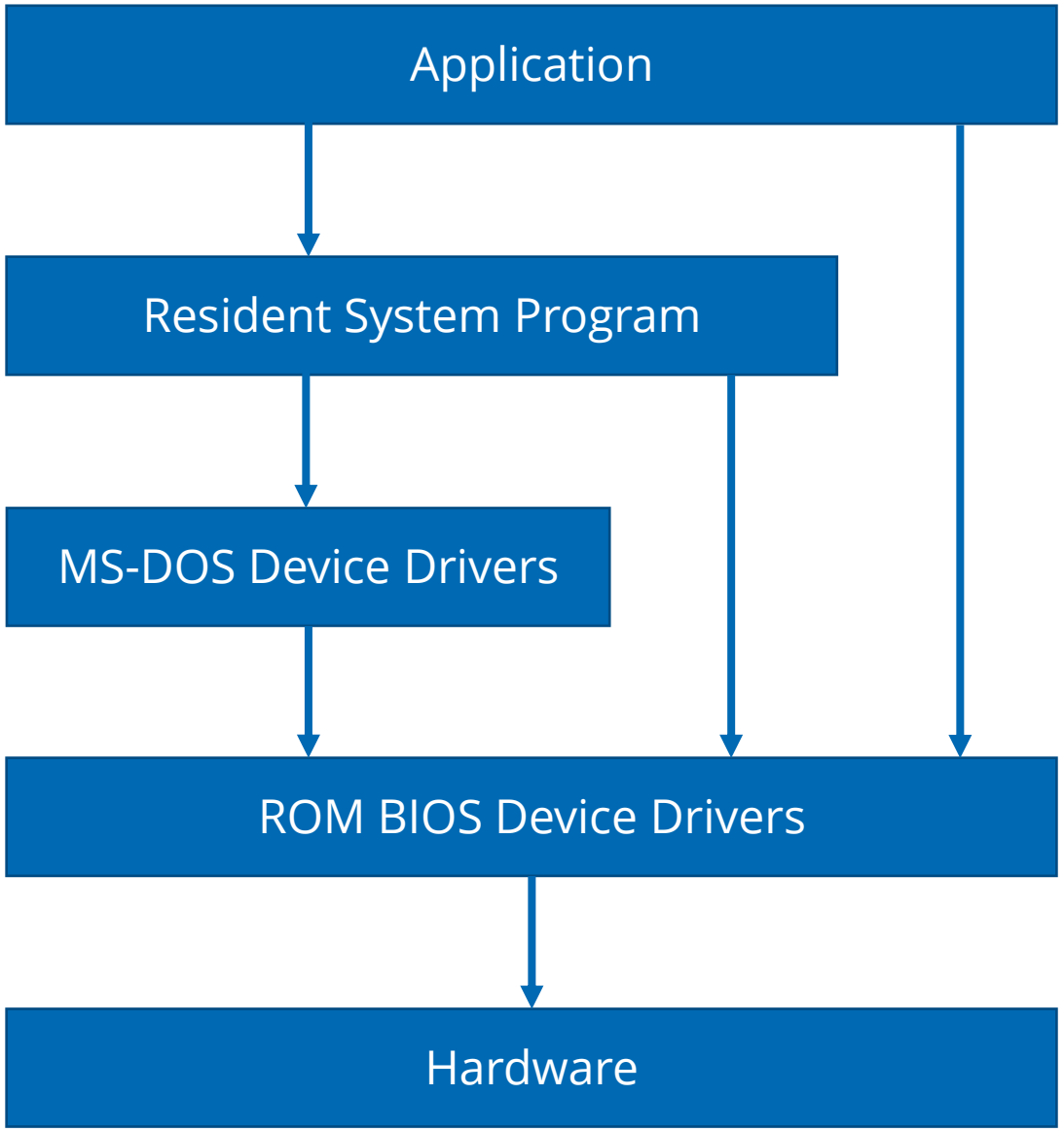
1. Historie (von DOS bis Windows 11)
2. Lizenz-Editionen (am Beispiel Windows 10)
3. Systemarchitektur (Windows NT)

Historie


THIS IS BILL GATES
COUNTING TO TEN
1. 2. 3. 95. 98. NT. 2000. XP. VISTA. 7. 8. 10

MS-DOS

- 12. August 1981
- Microsoft Disk Operating System
- Aufgekauft von Seattle Computer Products als 86-DOS
- Lizensiert an IBM und 70 andere Firmen
- Versionen 1-6
- Nur für x86
- Single User
- Keine Rechte Staffelung
- Multitasking ab Version 4
- Nur Command Line Interface

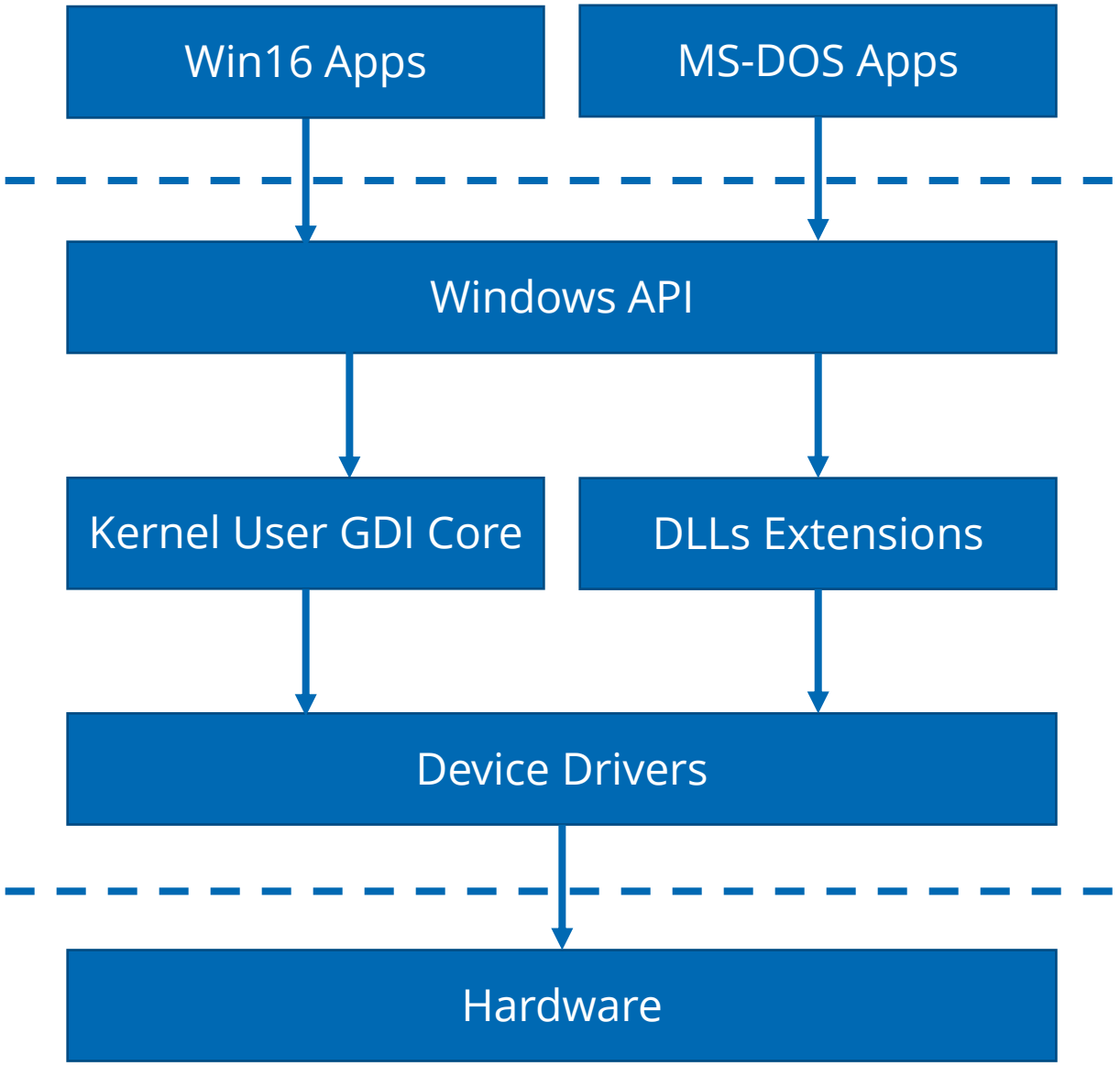


MS-DOS

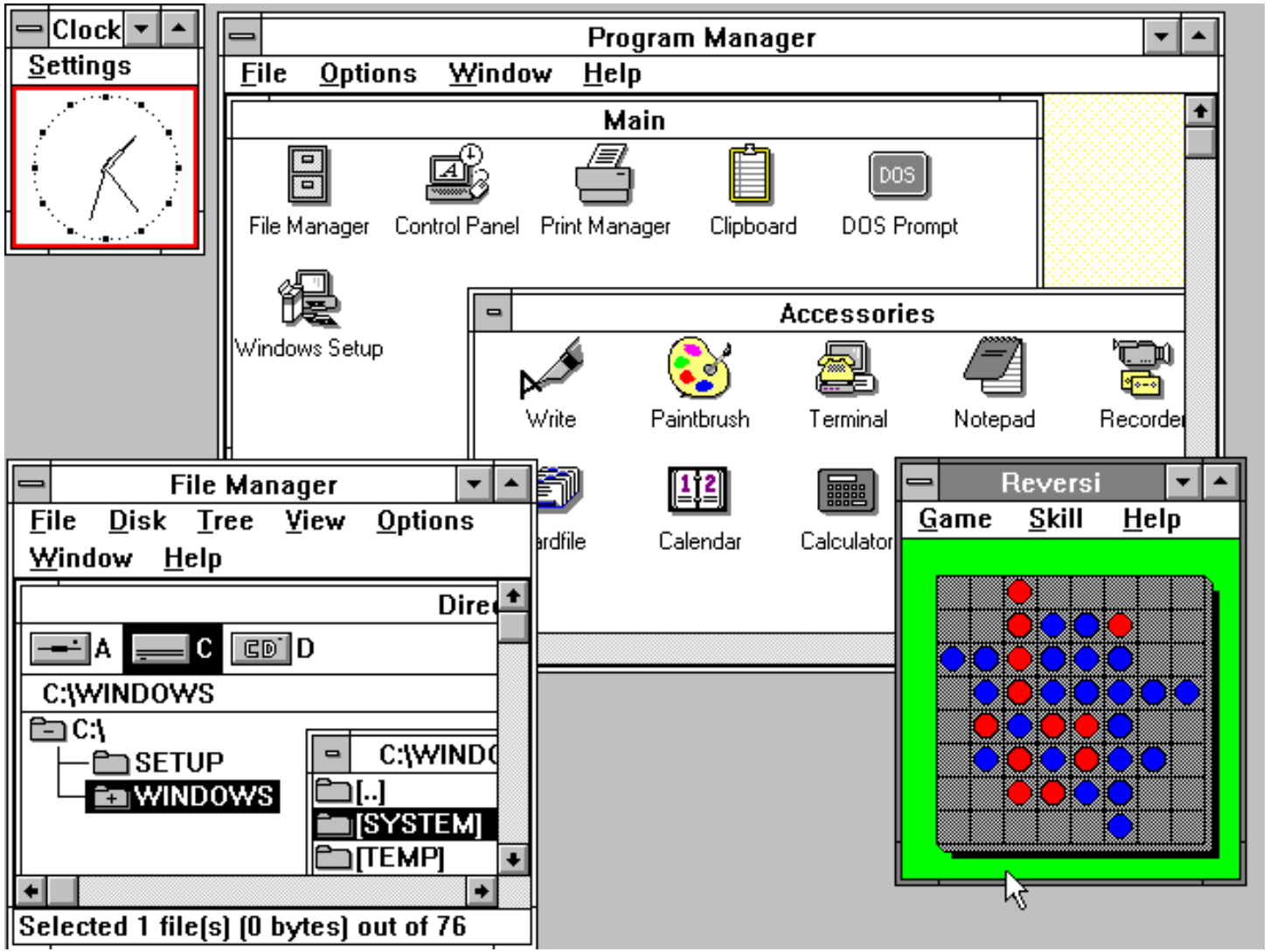
```
Seattle DOS version 3.1
Command v 3.10 (C)Copyright Microsoft Corp 1981, 1985
Copyright 1984, 1985 Falcon Technology, Inc.

Current date is Sun  1-07-2018
Enter new date (mm-dd-yy):
Current time is  0:36:35.75
Enter new time:

A>dir /w

 Volume in drive A is SEADOS31MAS
 Directory of  A:\

COMMAND  COM    ASSIGN   COM    ATTRIB   EXE    BACKUP   COM    BADSPOT  COM
CHKDSK   COM    DEBUG    COM    DISKCOPY COM    EDLIN    COM    EXE2BIN  EXE
FC       EXE    FDISK    COM    FIND     EXE    FORMAT   COM    GRAPHICS COM
JOIN     EXE    LABEL    EXE    LINK     EXE    MODE     COM    MORE     COM
MOVE     COM    PRINT    COM    RECOVER  COM    RENDIR   COM    RESTORE  COM
SHARE    EXE    SHIPDISK COM    SORT     EXE    SUBST    EXE    SYS      COM
TREE     COM    WHERE    COM
       32 File(s)    100352 bytes free

A>_
```

Windows 1-3

- 1985-1990
- Graphische Oberfläche für MS-DOS
- Virtual Memory Management
- Protected Mode zum Umgehen von Virtual Memory
- Workgroups für Peer-to-Peer Data Share
- Windows 3.0 erste populäre Version von Windows
  → Akzeptanz von GUIs
- Einführung der Registry in Windows 3.1

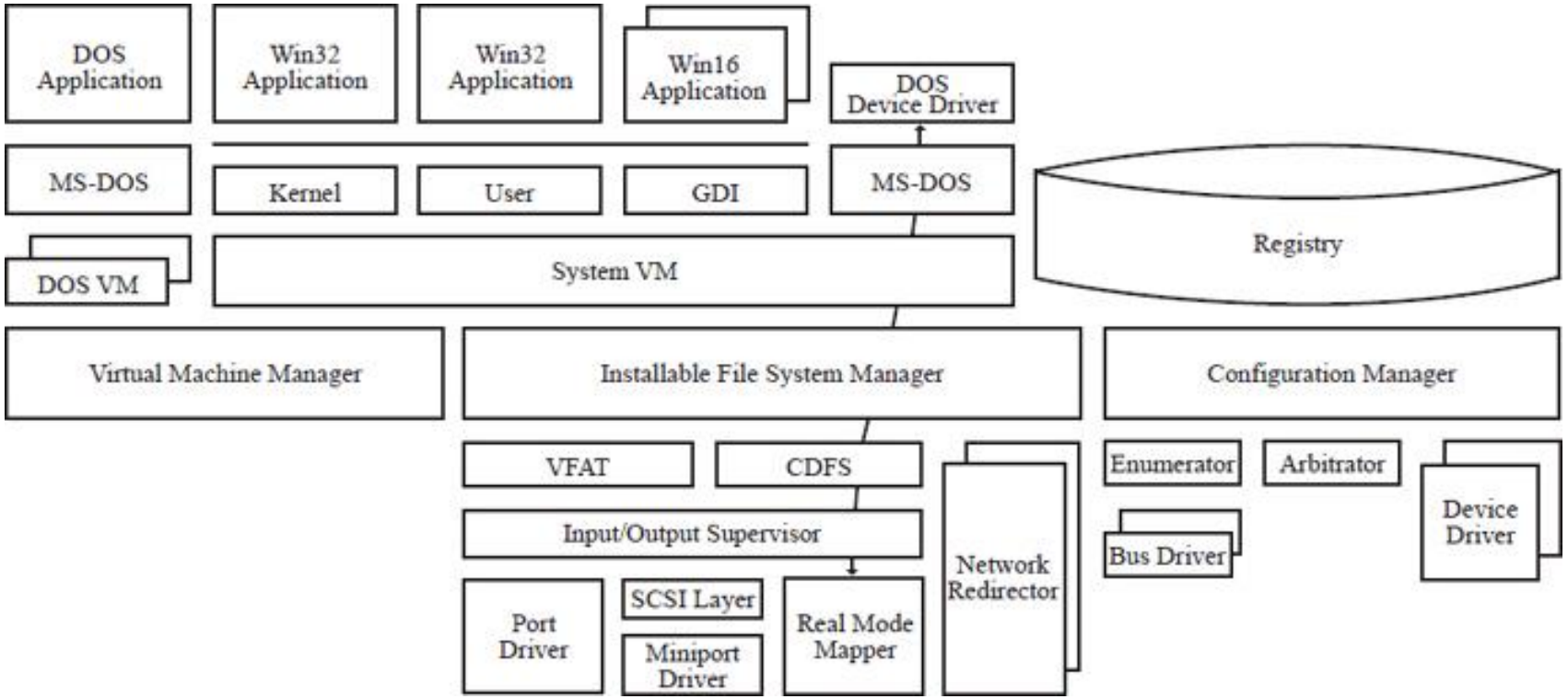


Windows 1-3

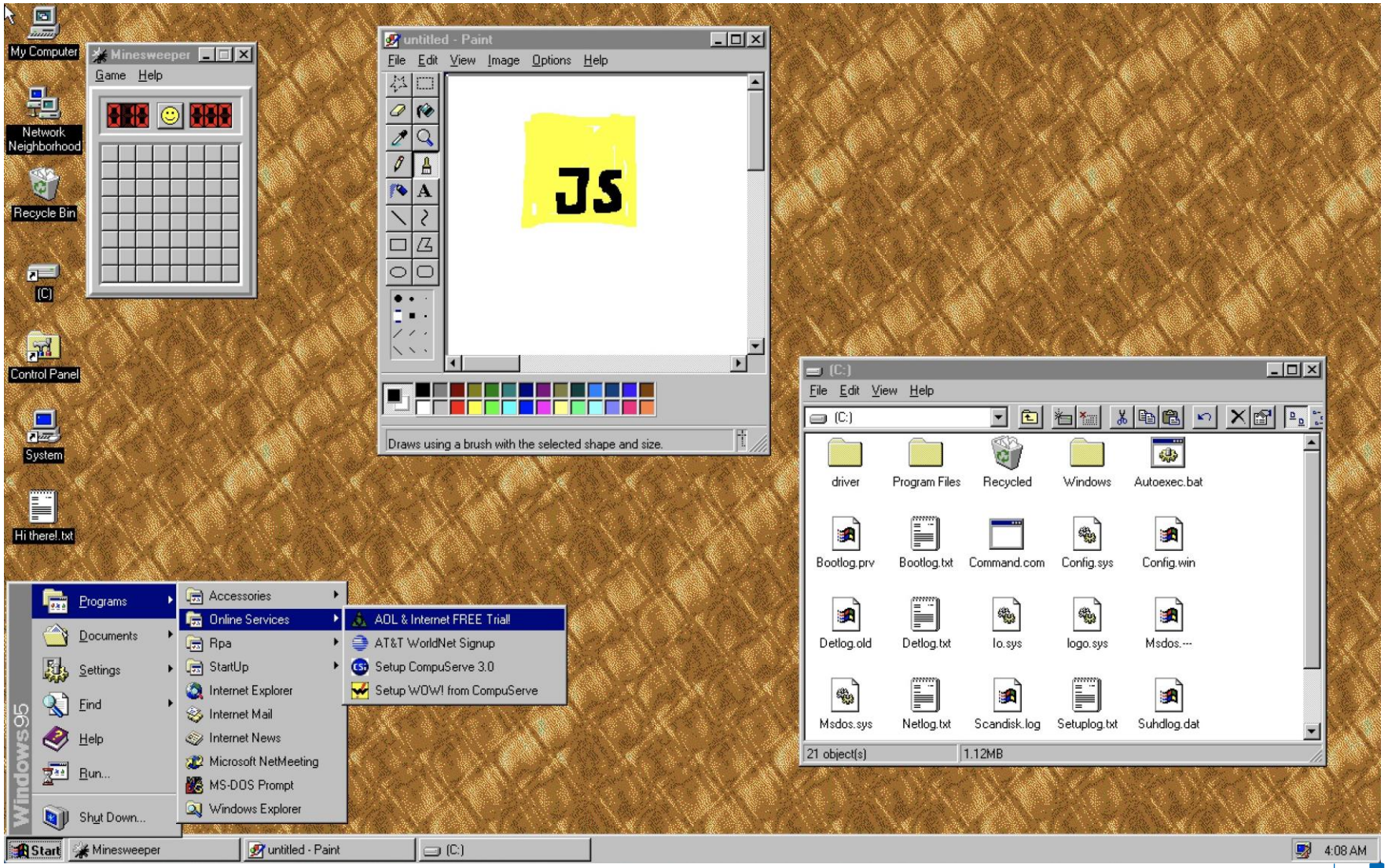


Windows 95

- August 1995
- MS-DOS basiert
- 32 Bit Support
- 255 Zeichen lange Dateinamen
- Startmenü und Taskbar
- TCP/IP-Stack standardmäßig
- Internet Explorer
- DirectX-API für Spiele

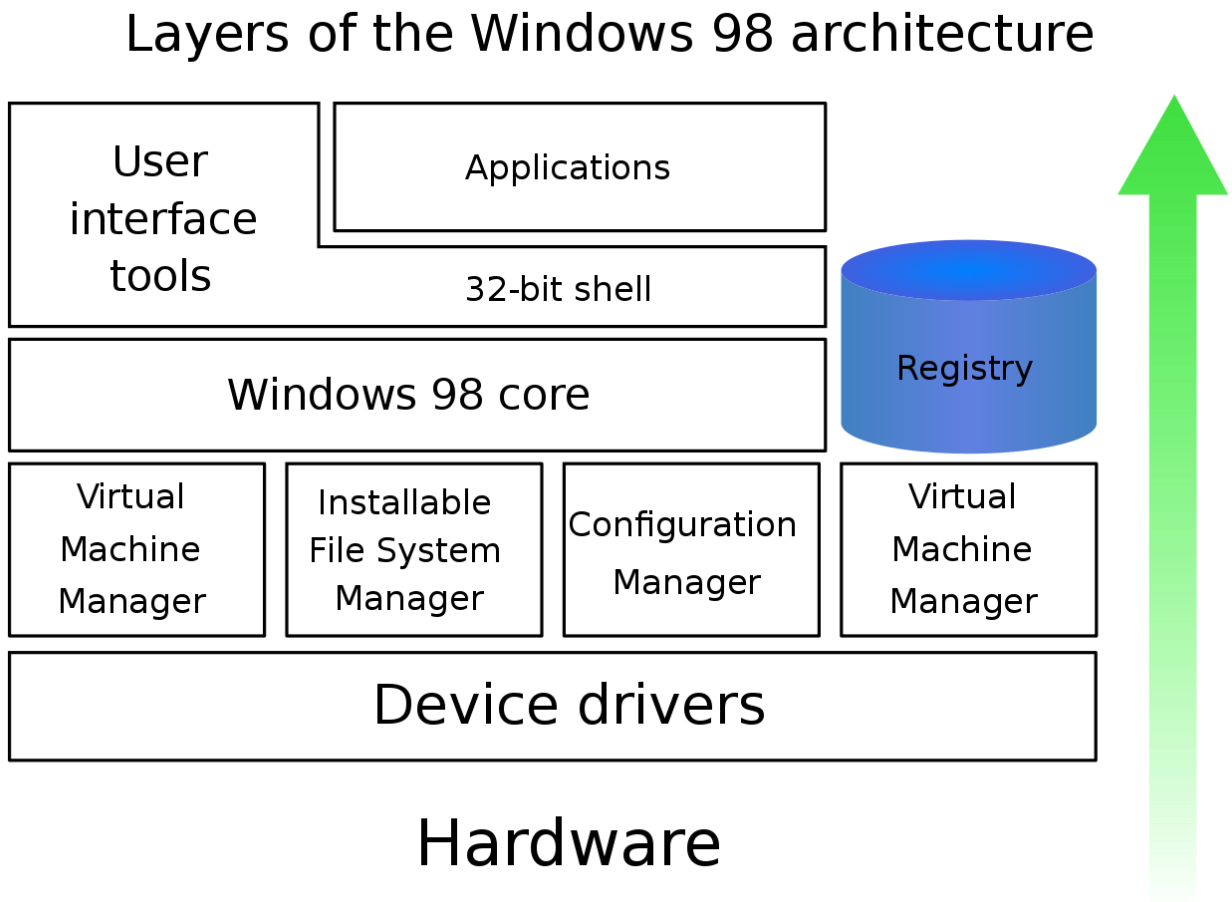


Windows 95



Windows 98

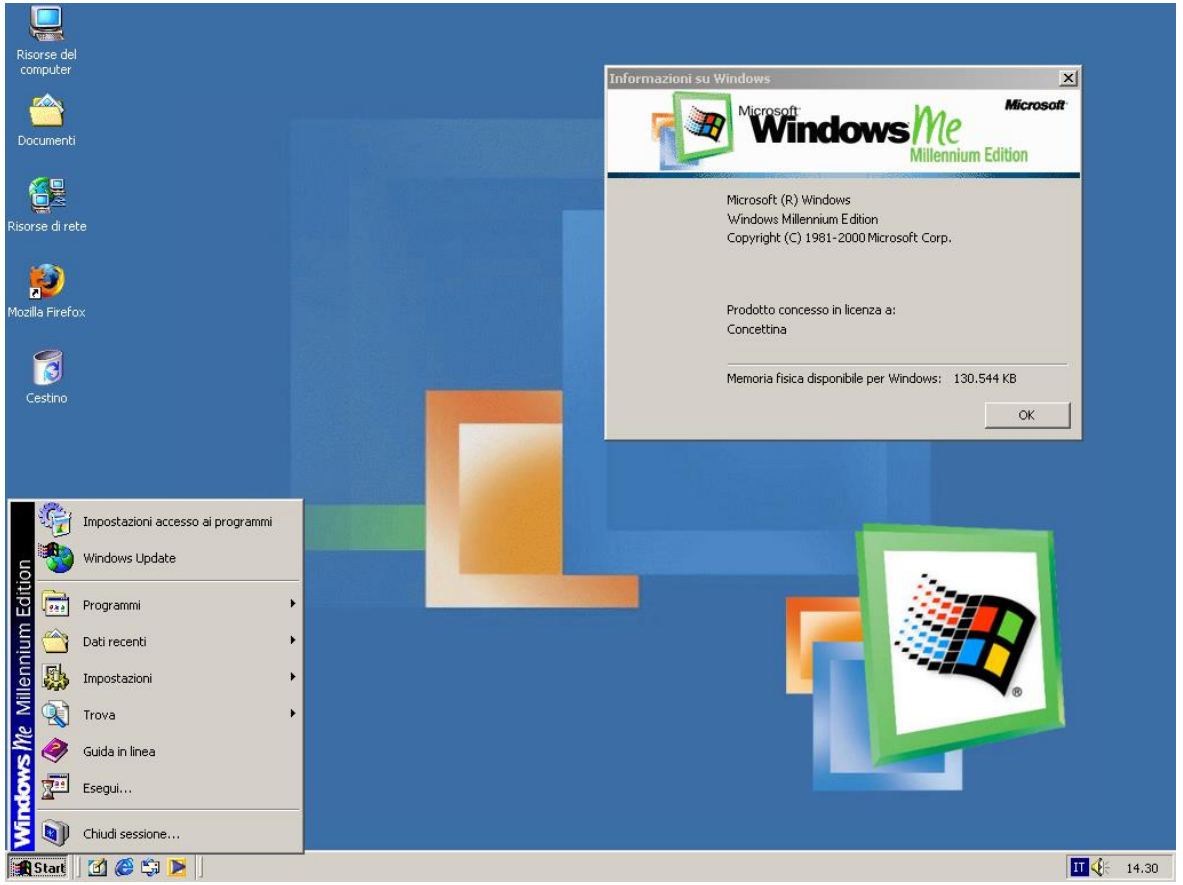
- Juni 1998
- Basiert auf Windows 95
- Windows Driver Module
- Internet Explorer 4.0 integriert
- Outlook integriert
- Erweiterter USB-Support
- Navigationshistorie
  - Zurück
  - Vorwärts



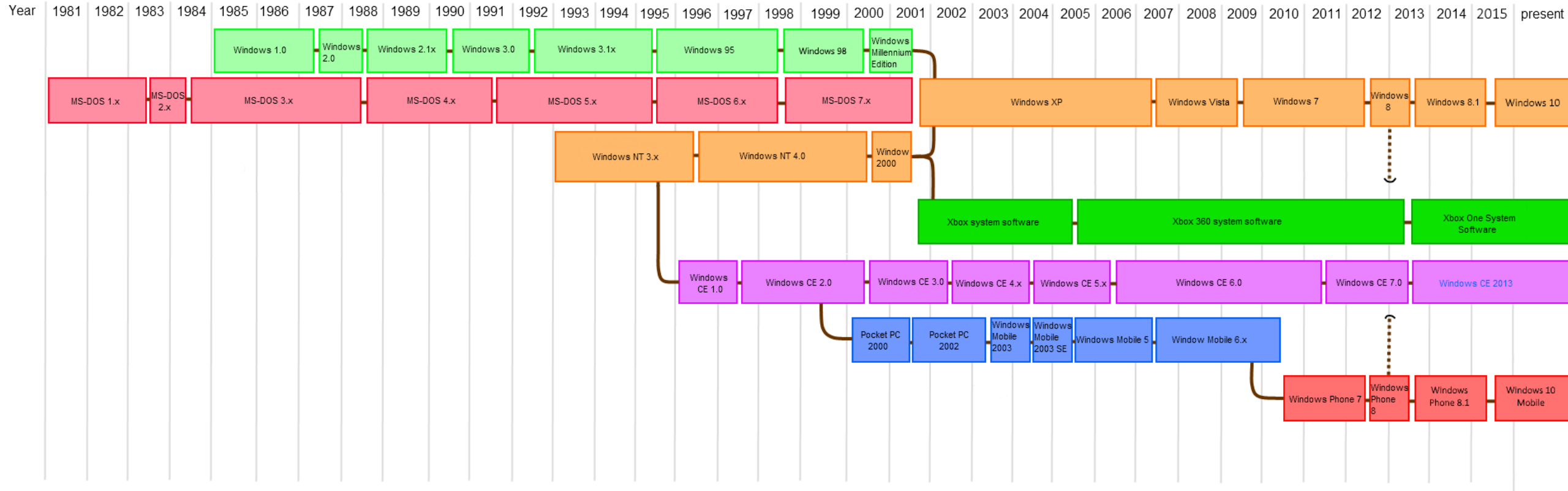
Windows 98

Windows ME

- September 2000
- Verbesserte Multimediafunktionen:
  - Windows Movie Maker
  - Windows Media Player
  - Windows DVD Player
- Optimierung der 9x Reihe
- Plug and Play Ausrichtung
  - API-Schnittstellen für Kameras und Scanner
  - USB-Storage Support
  - UPnP
  - Network Crawling für lokal Shares
- Weniger beliebt, da sehr instabil

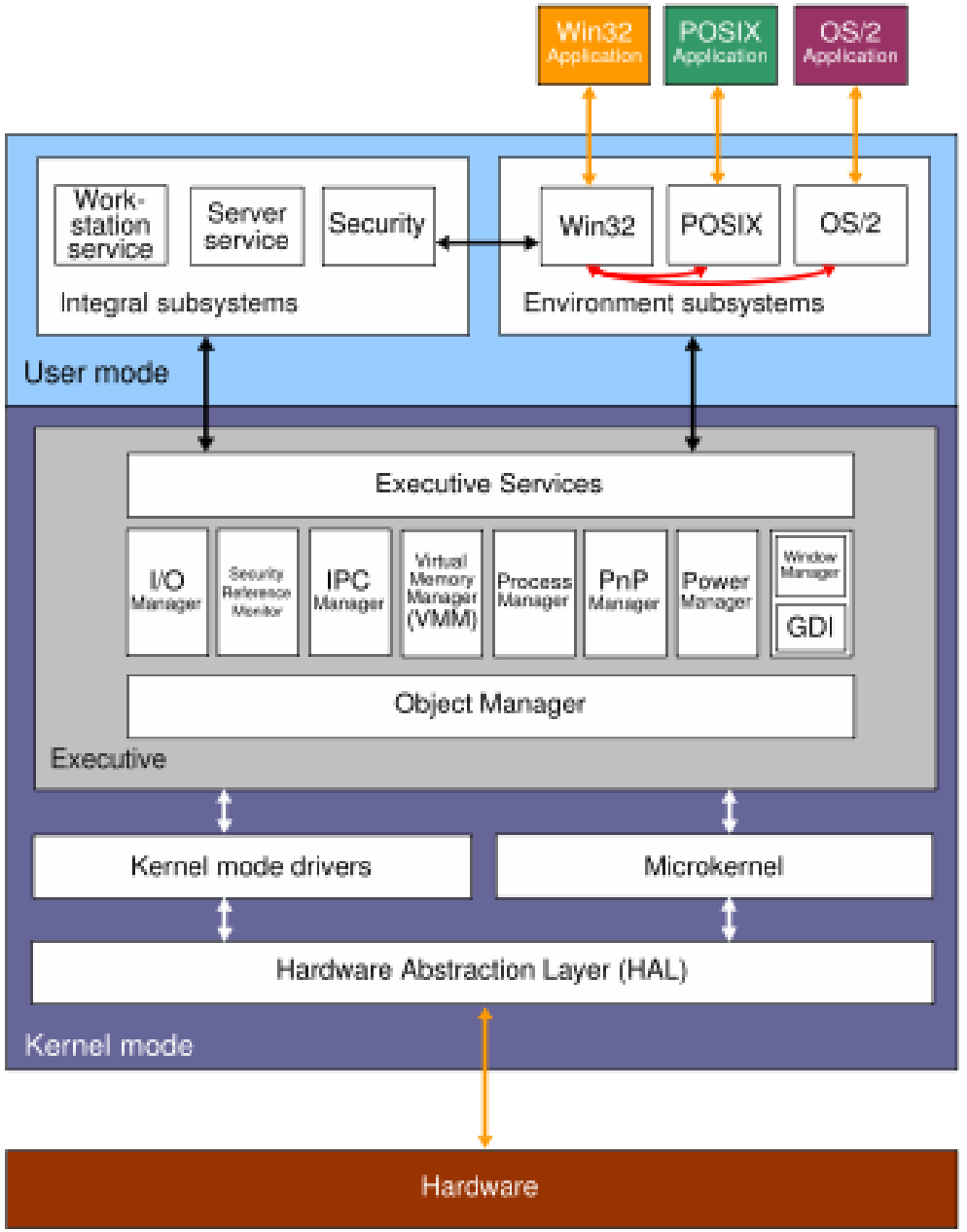


Windows NT

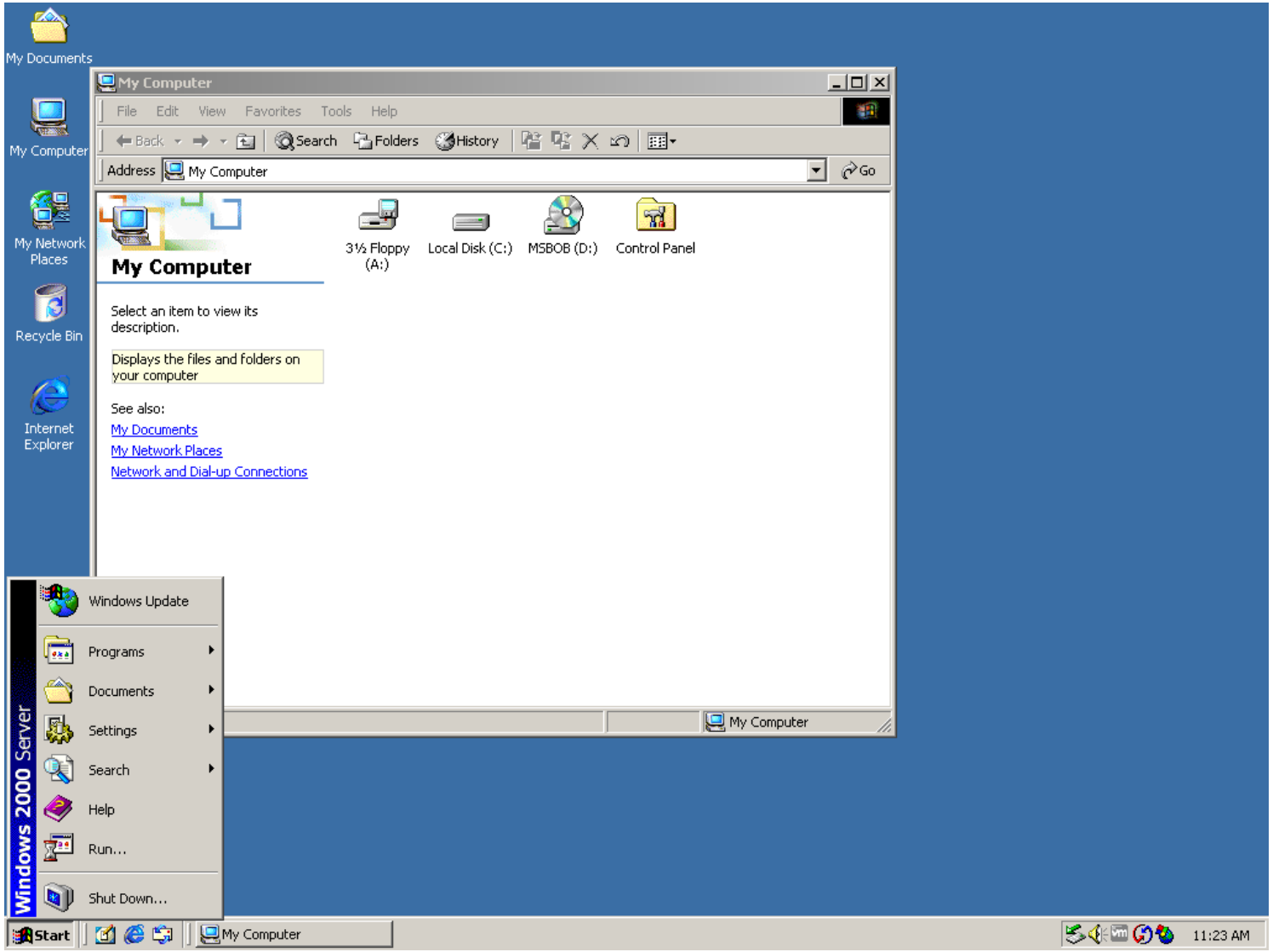


Windows 2000

- Februar 2000
- Neue NT-Architektur
- Architekturbasis bis heute
- Business- und Homeorientierung
- Einführung von Active Directory
- Encryption File System
- Plug and Play Driver Orientierung
- Windows Driver Module
- Logical Disk Manager (Software RAID)
- Accessability Features (Screen Keyboard)

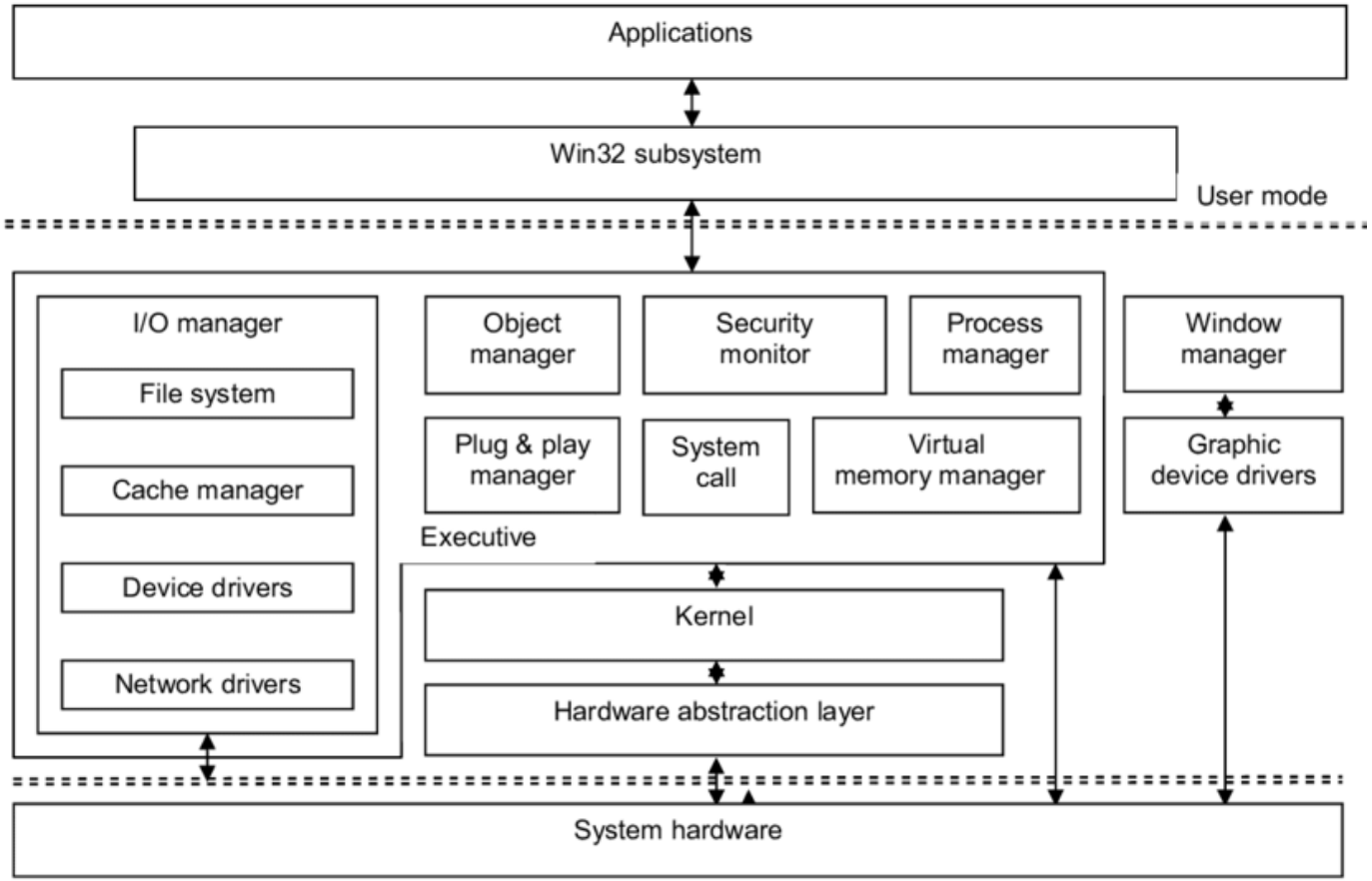


Windows 2000

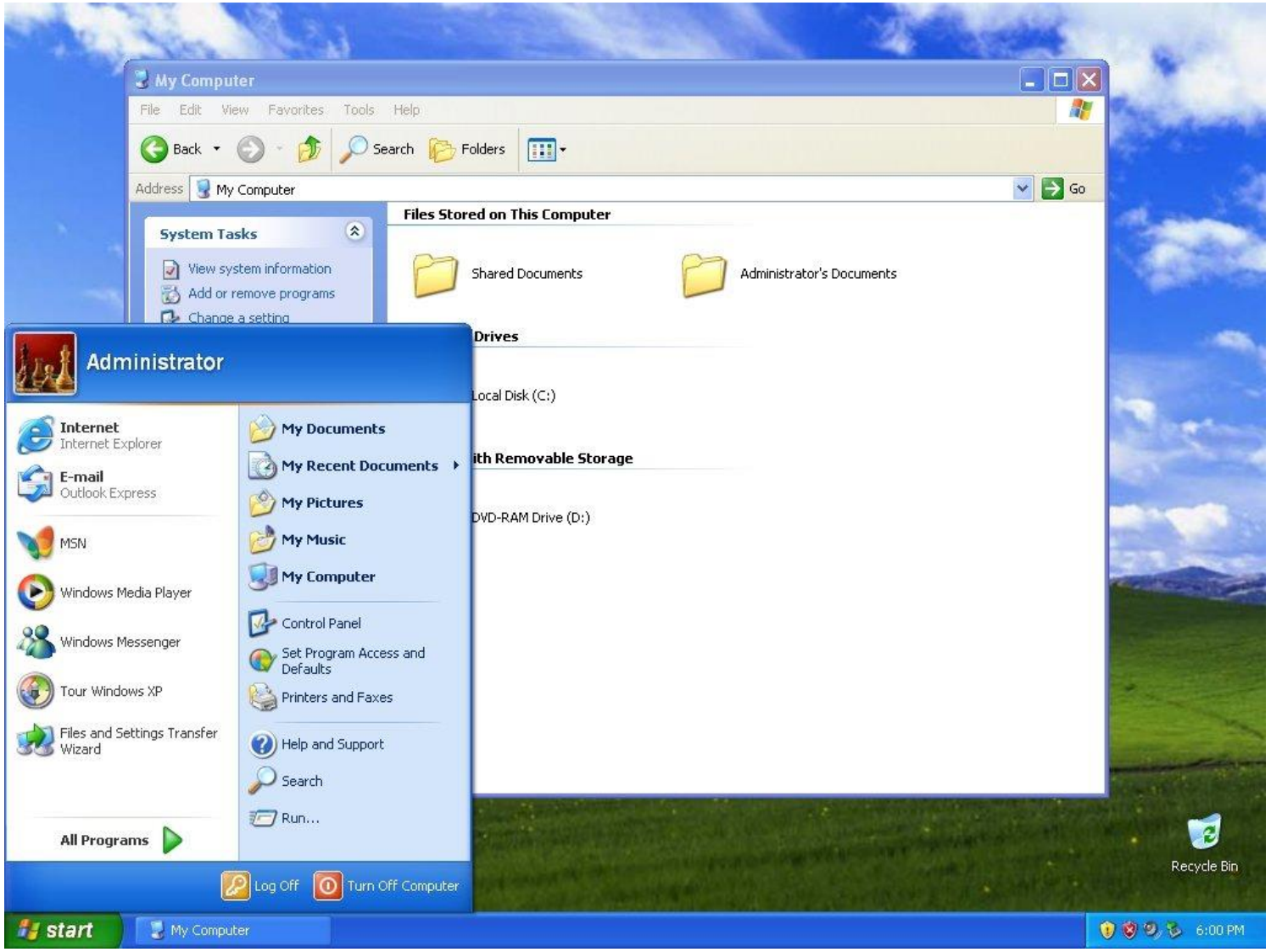


Windows XP

- Oktober 2001
- Architektur von NT und Programme von 9x-Serie
- Session Switching zwischen Users
- Logout erfordert kein Schließen der Programme
- Neues UI-Design
- Prefetching von Programmen für schnelleres Starten

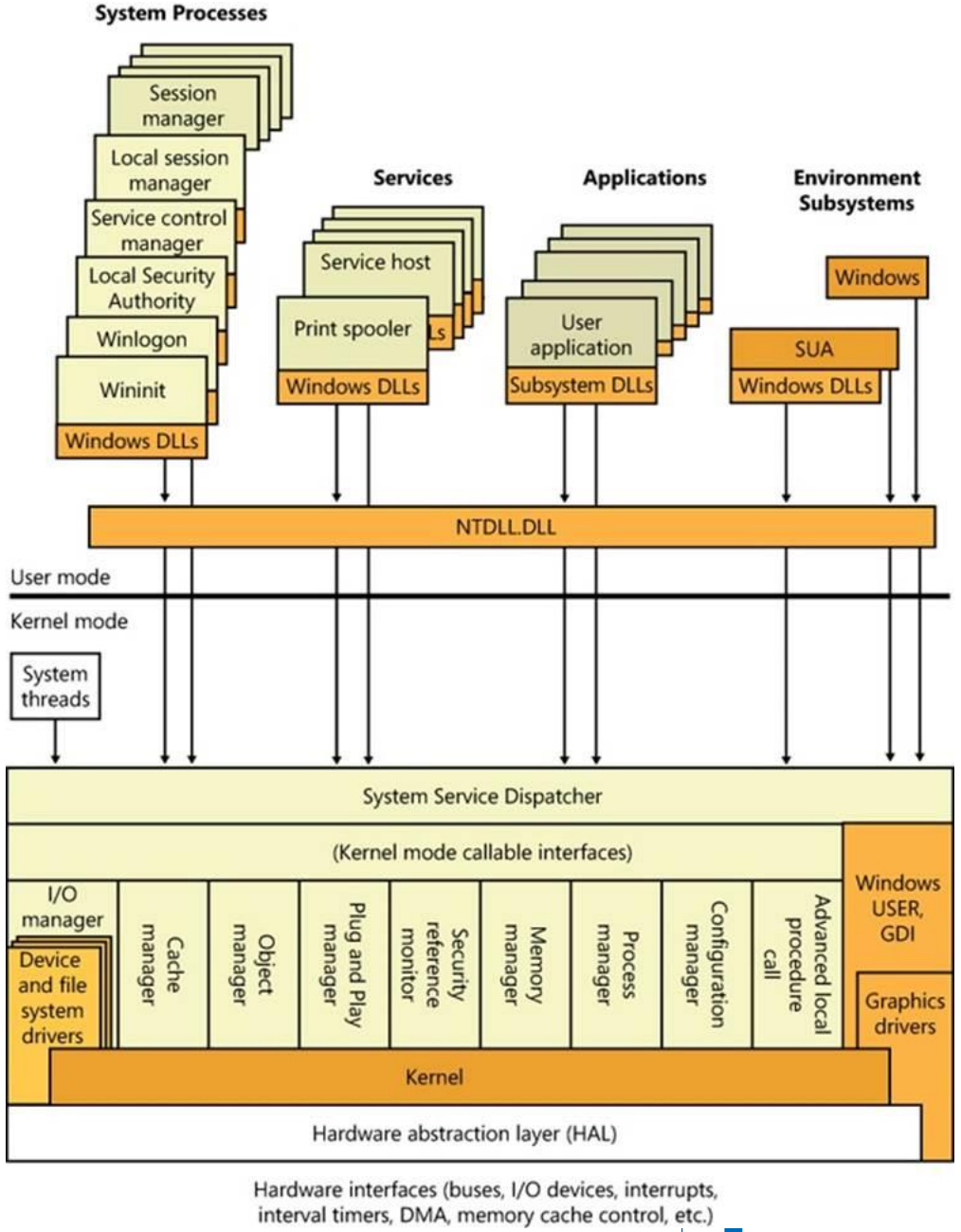


Windows XP



Windows Vista

- Januar 2007
- Graphische UI mit Transparenz (Aero-Design)
- User Account Control (Rechteeinschränkung des normalen Users nach Unix Vorbild)
- Windows Defender
- Shadow Copy
- Spracherkennung
- Voller IPv6-Support
- BitLocker Drive Encryption
- Code / Heap Integrity Checks
- Address Space Layout Randomization

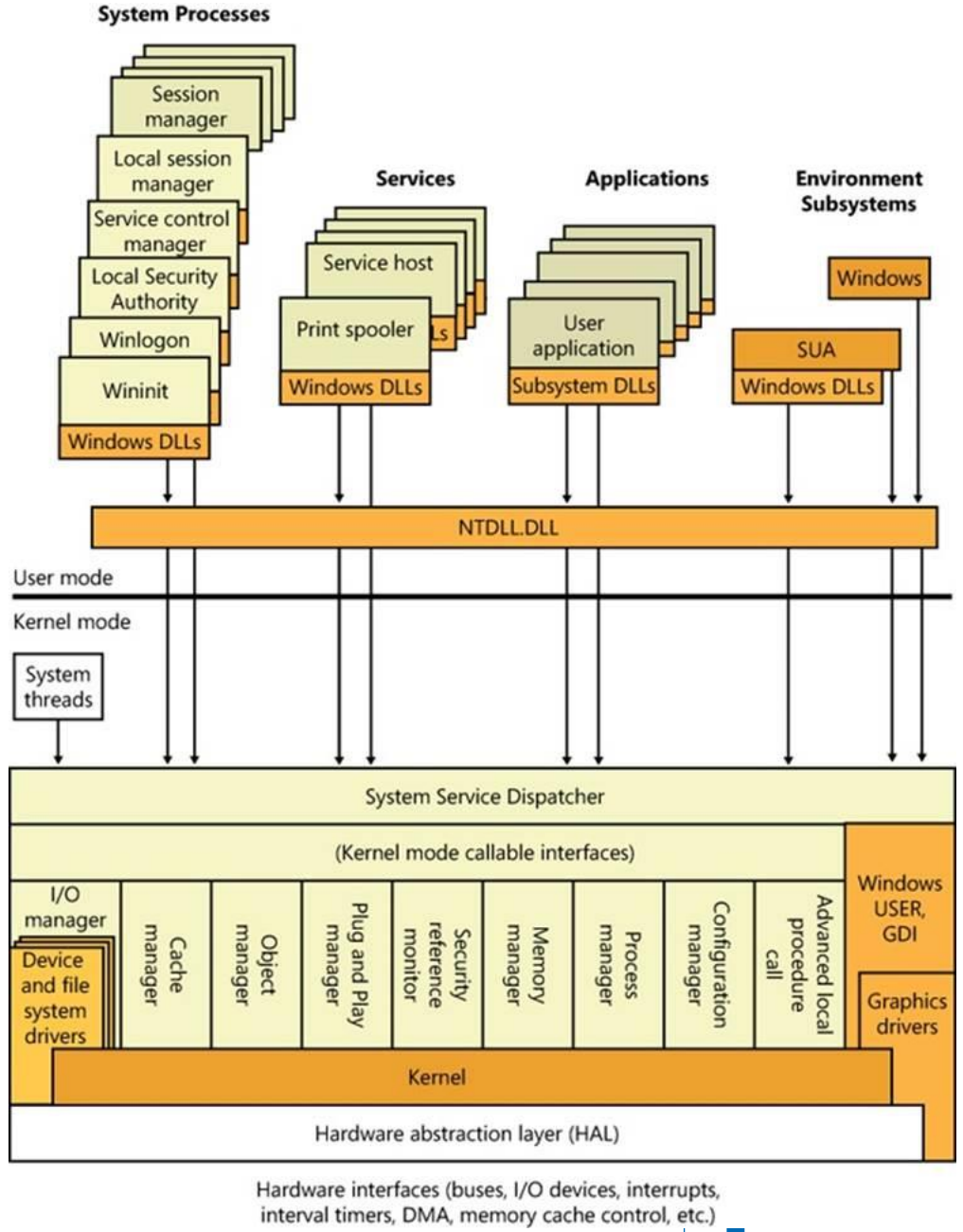


Windows Vista

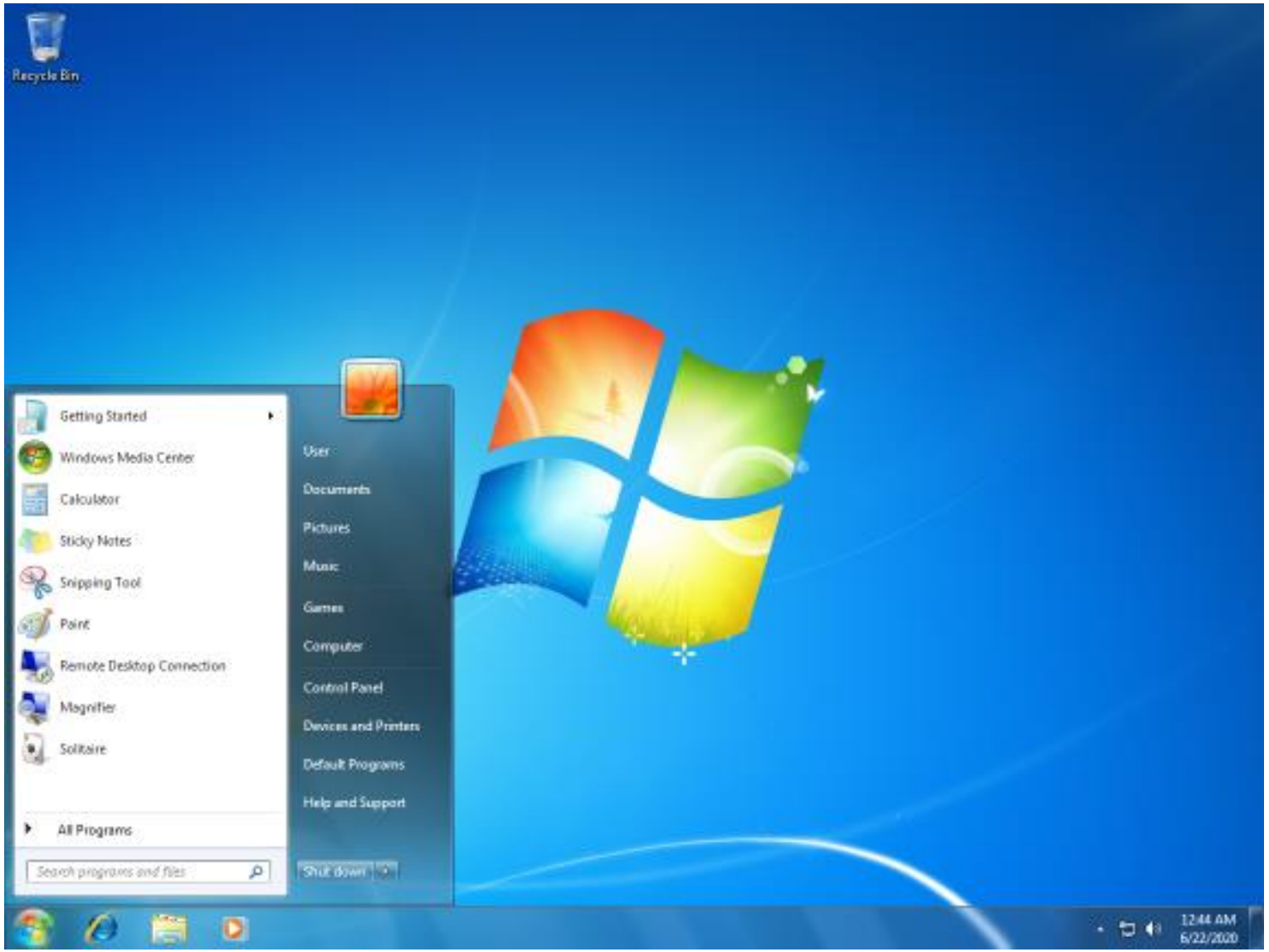
Windows 7

- Oktober 2009
- Besseres Vista (Leistung und Benutzerfreundlichkeit)
- Handschrifterkennung
- Performance besonders auf Multicore CPUs optimiert
- Windows Power Shell
- Support für Virtual Hard Disks
- Von Microsoft Signierte Programme erfordern keine Sicherheitsfreigabe

➢ Weniger Sicherheits-Popups

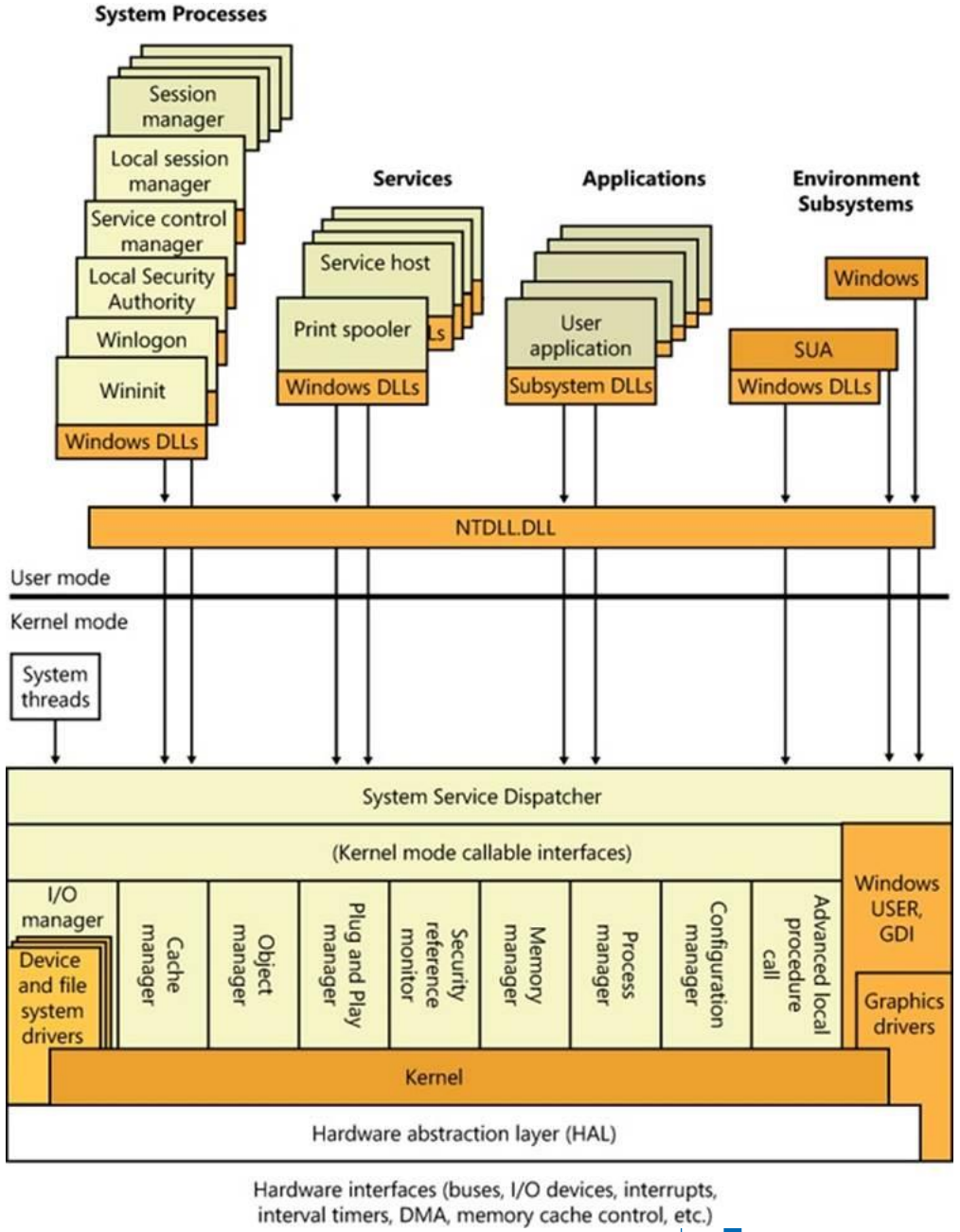


Windows 7



Windows 8

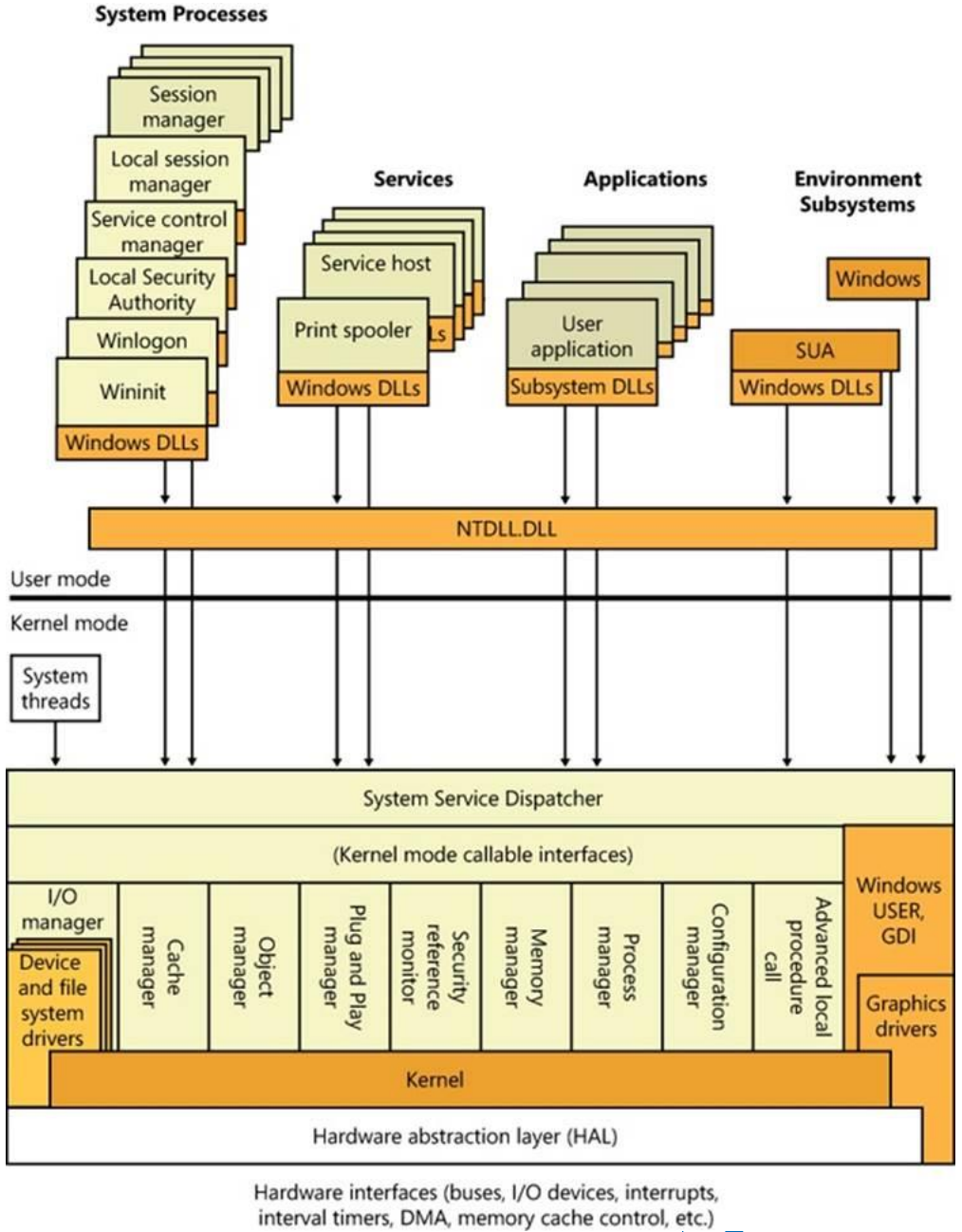
- Oktober 2012
- Userinterface auf Touch Optimiert
- UEFI Secure Boot
- Windows RT für ARM Architektur
- Windows to Go (LiveUSB)
- USB 3.0 Support
- PIN und Picture Authentication
- Cloud Support mit Microsoft Account
- Einführung Windows Store



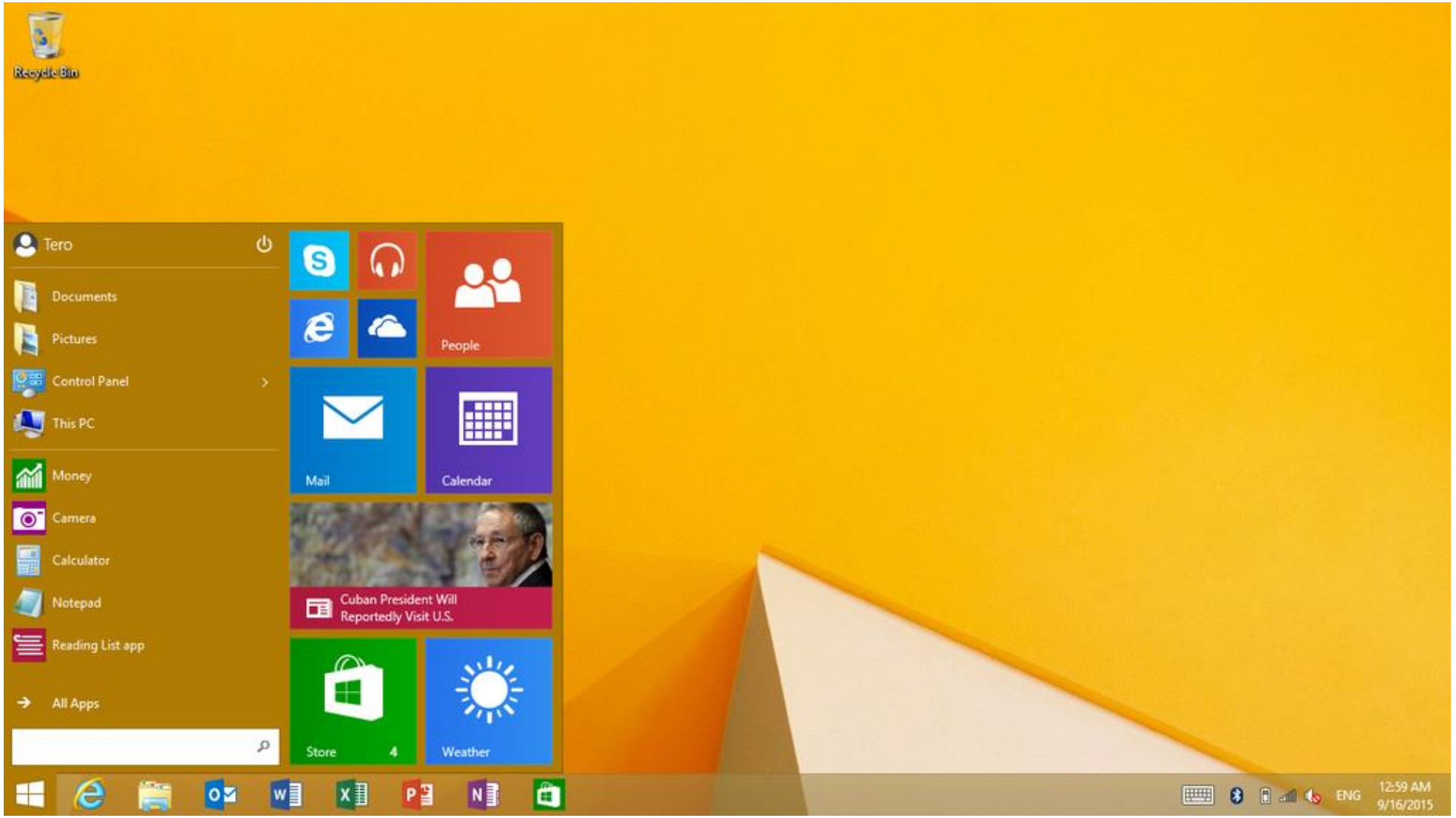
Windows 8

Windows 8.1

- Oktober 2013
- Adressierung von Benutzerkritik
- Startmenü wieder nativ aktiv
- Performance von Cloud-Diensten verbessert
- OneDrive Integration
- Transparent Device Encryption mit Bitlocker
- KeyStorage in AD oder MS-Cloud
- Intrusion Detection System für Windows Defender

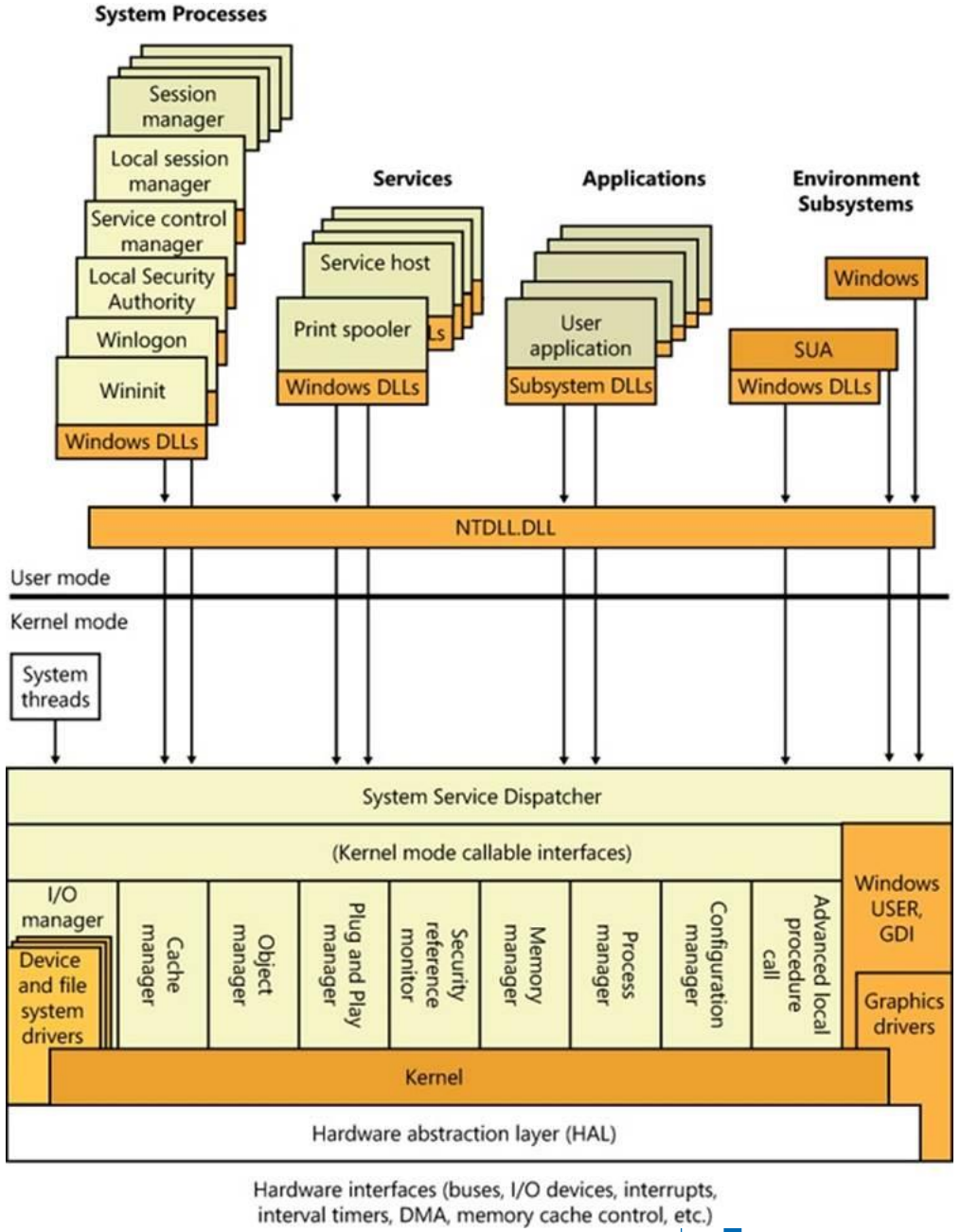


Windows 8.1

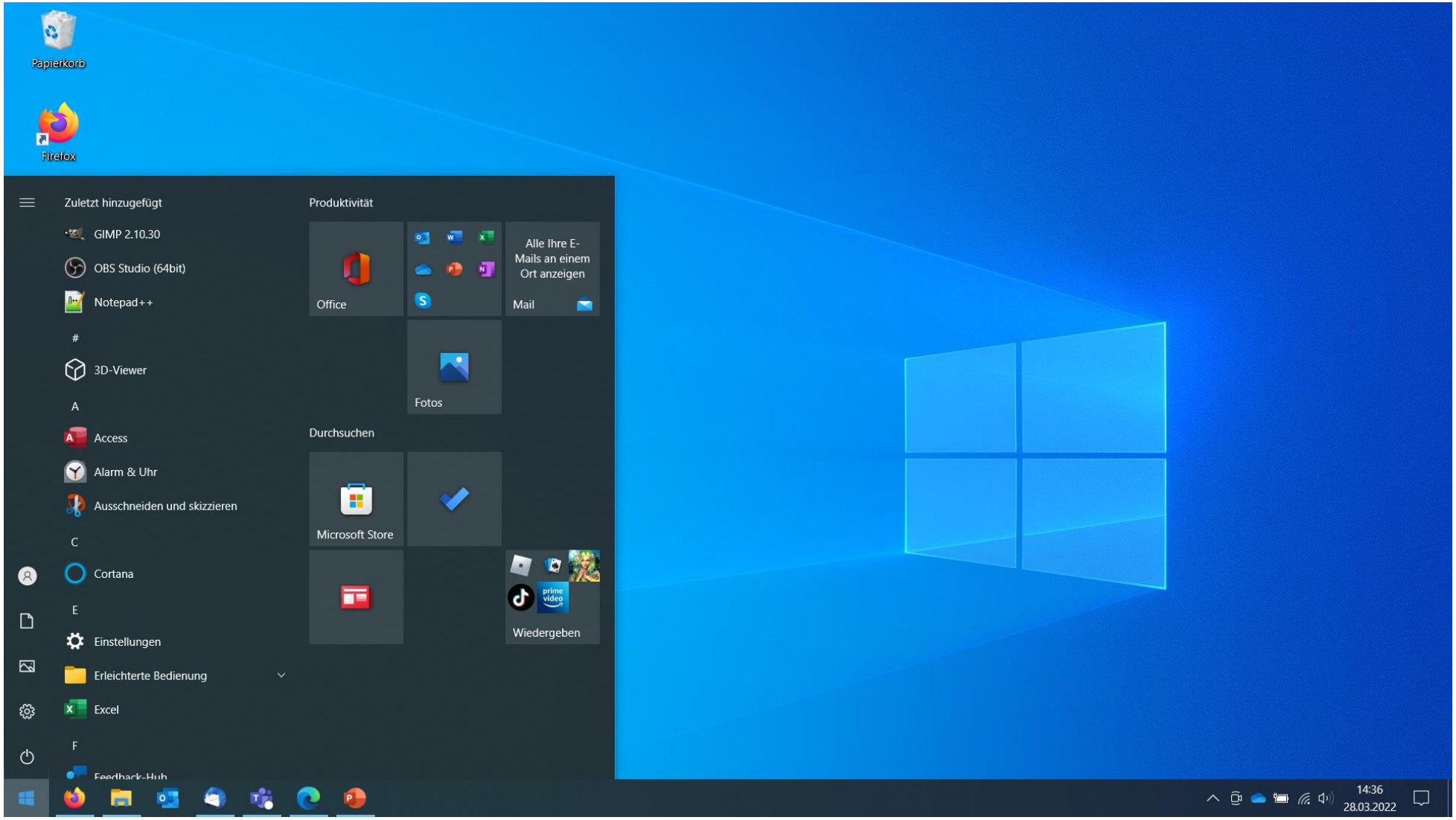

Recycle Bin
Tero
Documents
Pictures
Control Panel
This PC
Money
Camera
Calculator
Notepad
Reading List app
All Apps
People
Mail
Calendar
Cuban President Will Reportedly Visit U.S.
Store
4
Weather
ENG
12:59 AM
9/16/2015

Windows 10

- Juli 2015
- Cortana Personal Assistant
- Xbox Live Integration
- Microsoft Edge ist Webbrowser
- User Activity Analysis und Fokus auf Werbung
- Microsoft Store (Appstore)
- UI optimiert für 2-in-1-PCs (wie Microsoft Surface)
- Gesichtserkennung als Authentifizierung
- Windows Subsystem for Linux
- Bisher konstanteste Version von Windows in Bezug auf die Lebendauer

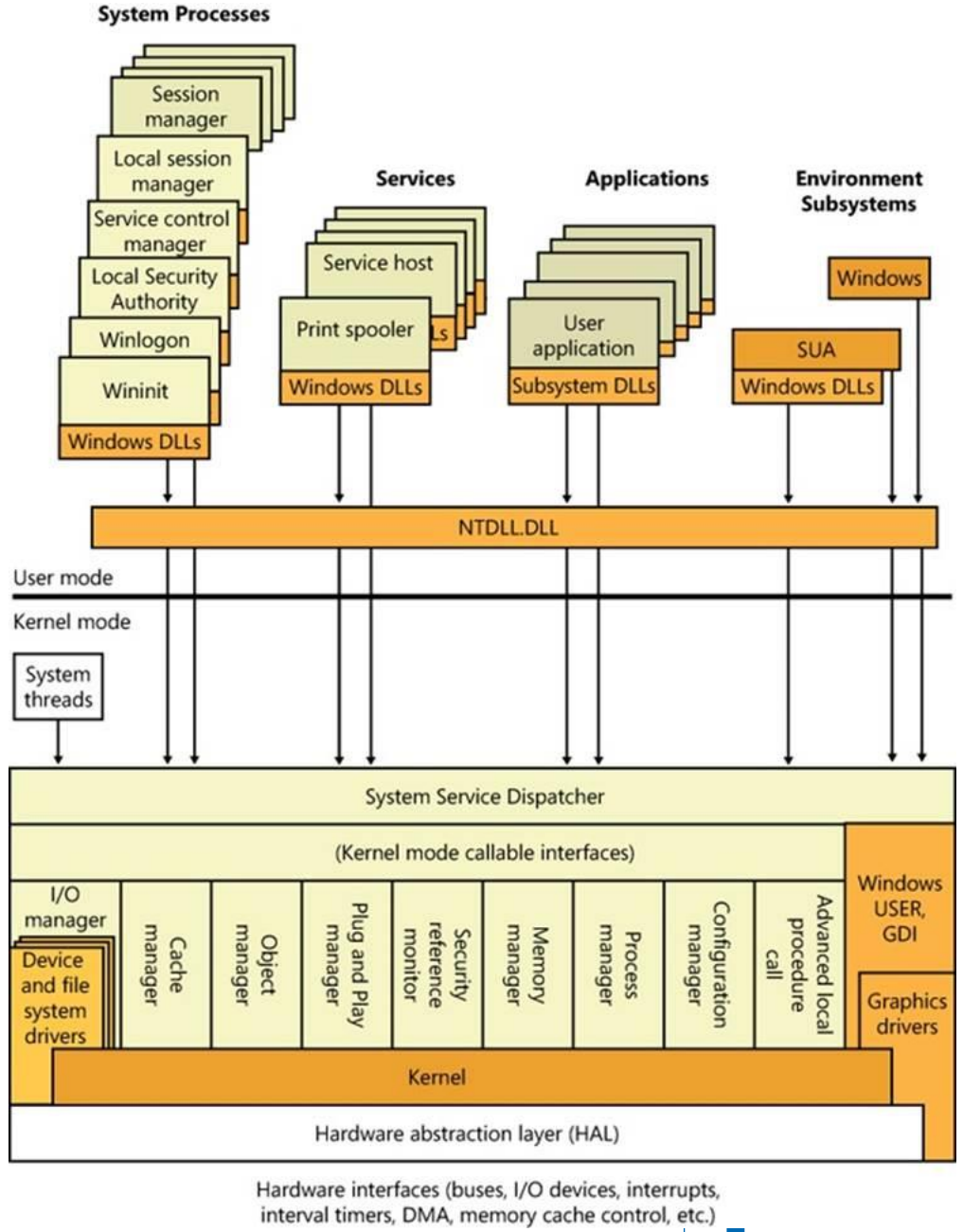


Windows 10

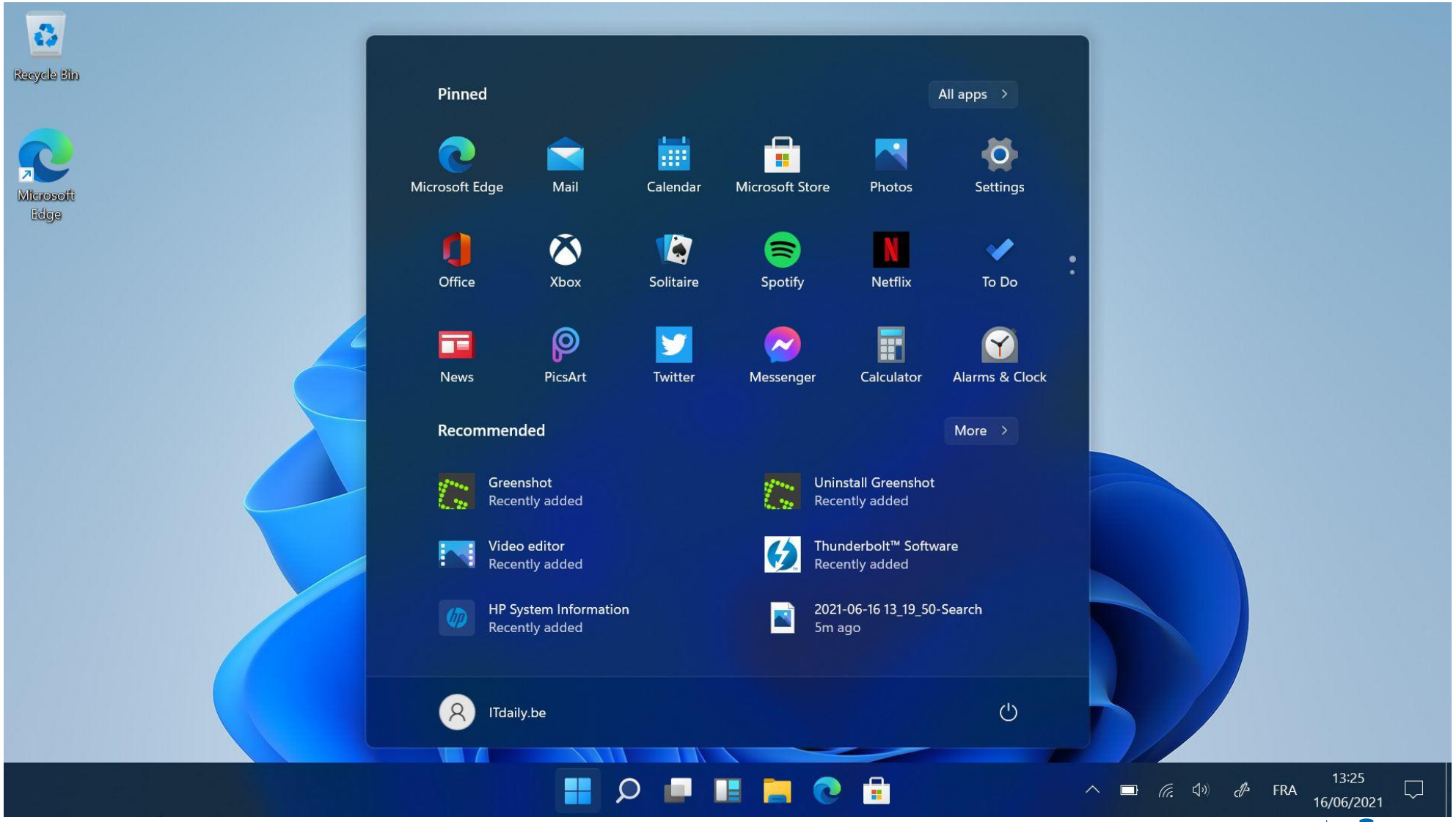


Windows 11

- Oktober 2021
- Nur noch 64 Bit
- Nur noch UEFI mit TPM
- Verbesserte Leistung und Energieeffizienz
- Schnelleres Booten
- Android Apps über Subsystem
- Microsoft Teams Integration
- Orientierung am Apple Design
- Virtuelle Desktops



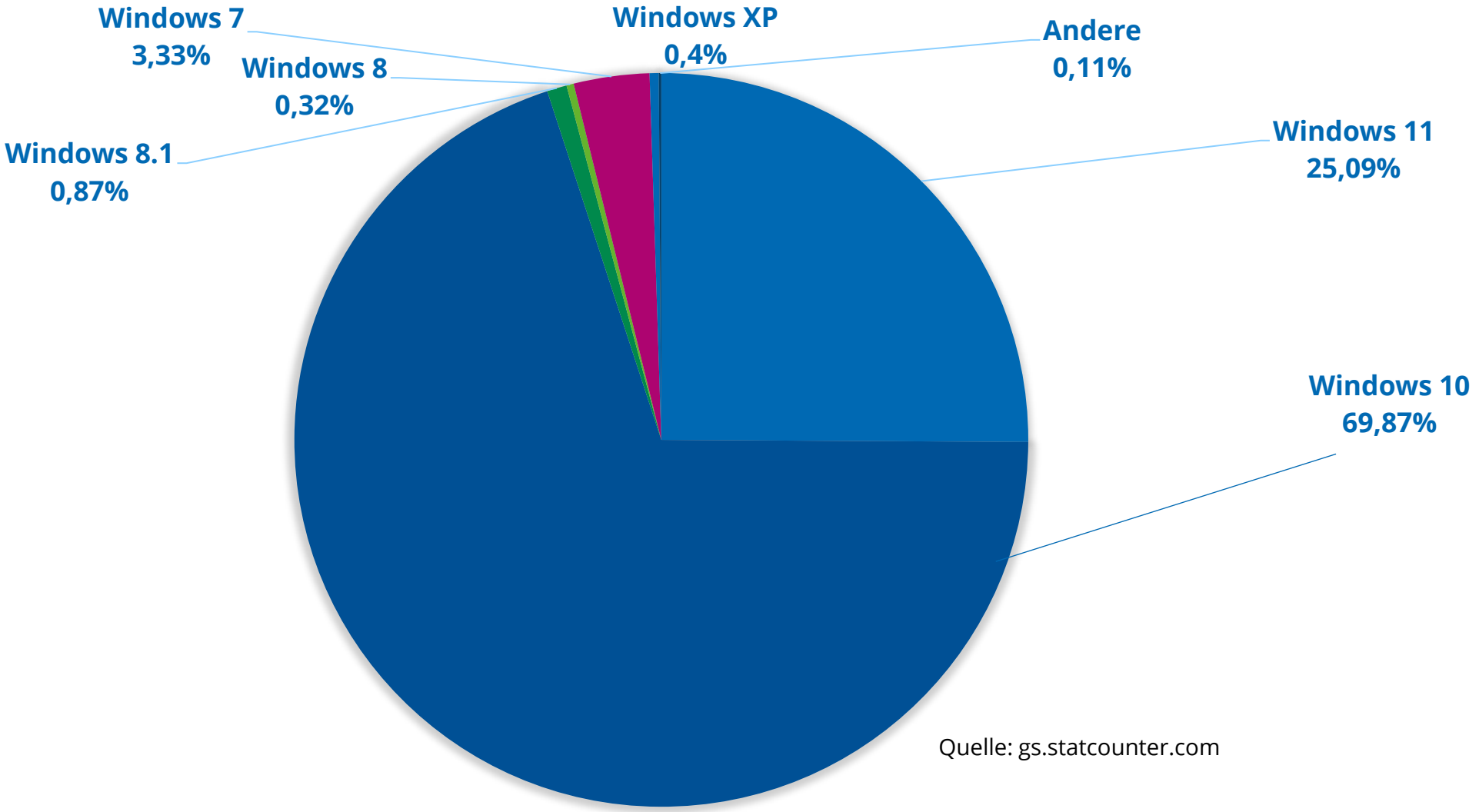
Windows 11



Windows Historie Zusammenfassung

- Ursprung in MS-DOS
- Windows 9x-Serie
- Windows NT
- Kürzliche Historie fokussiert auf Upgrades in
  - Oberfläche
  - Insbesondere Touch und Mobil
  - Subsysteme für andere OS
  - Userdaten als neues Geschäftsfeld
  - Clouddienste

Anteil Stand Mai 2024



Quelle: gs.statcounter.com

Windows 10 Editionen

Lizenzschlüsselarten

- Original Equipment Manufacturer (OEM)
  - Hersteller von Hardware installieren Windows vor
  - Lizenzschlüssel ist an exakt diese Hardware gebunden
- Retail
  - Kaufen im Laden / Händler
  - Lizenzschlüssel ist an Hardware der ersten Installation gebunden
  - Leichte Hardwareänderungen werden tolleriert
- Volumen Lizenz
  - Lizenz lässt sich mehrmals aktivieren
  - Volumen legt Häufigkeit fest

Heimgebrauch

Edition	Max RAM	Max CPUs	Max Cores	Hyper-V	Bitlocker	Long Term Service
Home	128GB	1	64	Nein	Nein	Nein
Pro	2TB	2	128	Ja	Ja	Nein
Pro for Workstations	6TB	4	256	ja	ja	Nein

- **Home** für den „normalen“ Nutzer
- **Pro** für Heimnutzer mit erhöhtem technischen Bedarf
- **Pro for Workstations** für Heimnutzer mit hohen Rechenbedarf

Enterprise

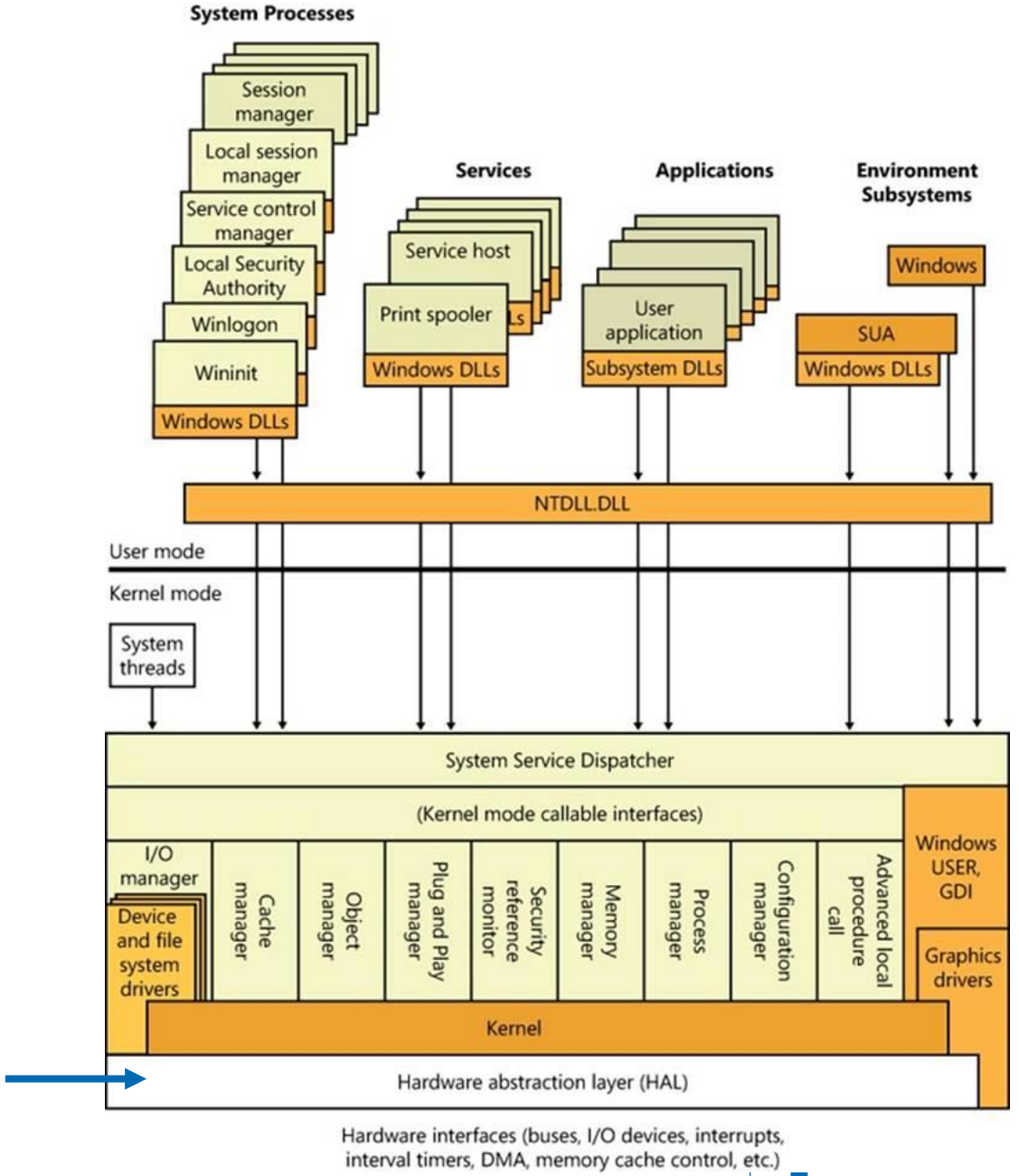
Edition	Max RAM	Max CPUs	Max Cores	Hyper-V	Bitlocker	Long Term Service
Education	2TB	2	128	Ja	ja	Nein
Pro (Education)	2TB	2	128	Ja	Ja	Nein
Enterprise	6TB	4	256	Ja	Ja	Nein
Enterprise LTSC	6TB	4	256	ja	Ja	Ja

- **Education** für Computer im Lehrinstitut
- **Pro (Education)** entspricht Heim-Pro-Version, Lizensiert von Lehrinstitut für Privat-PC von Schüler und Studenten
- **Enterprise** für „normalen“ Arbeitscomputer
- **Enterprise LTSC** für normalen Arbeitscomputer mit langem Security Support (Beispielsweise für auf Windows 10 speziell angepasste Software)

Systemarachitektur

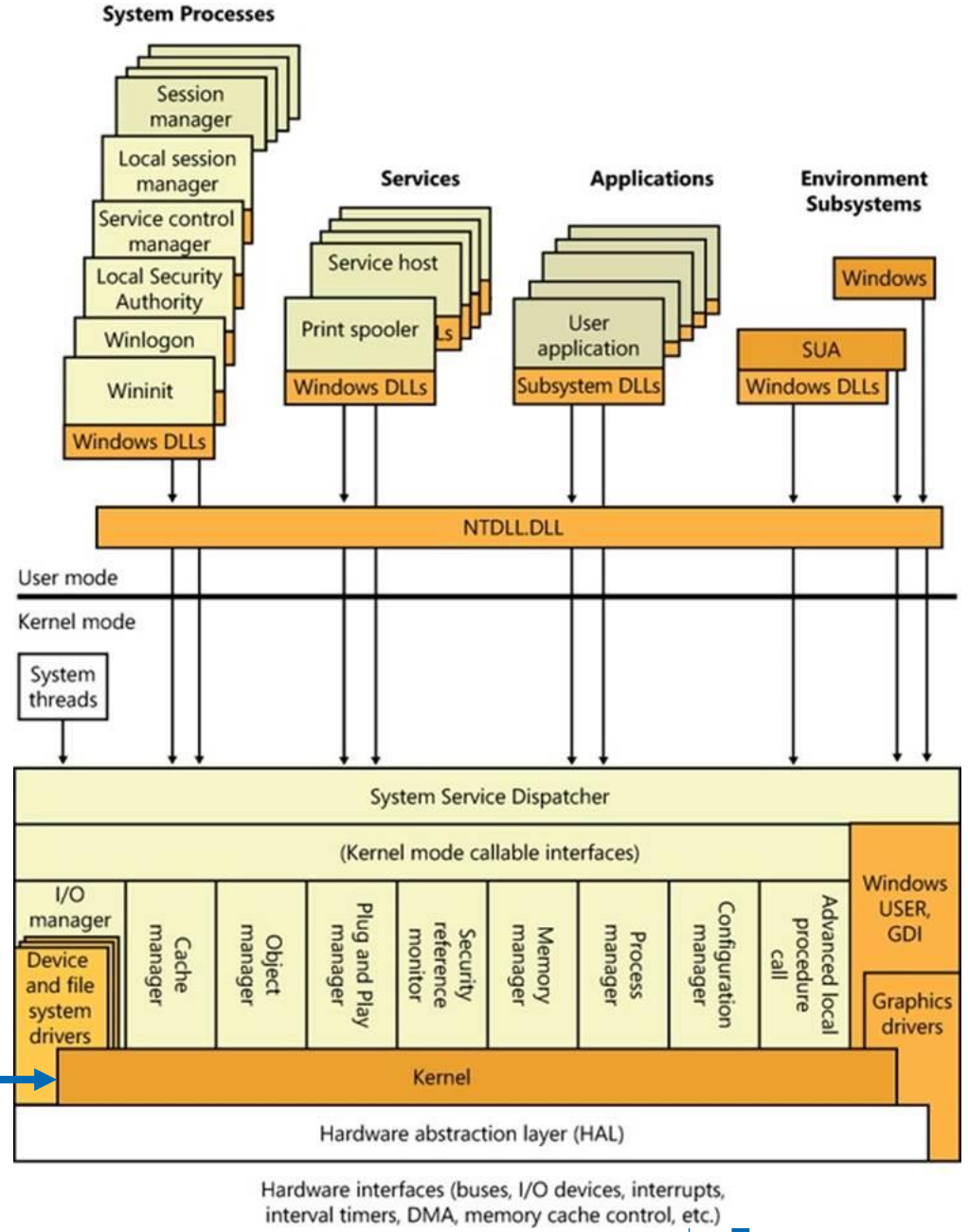
HAL

- Hardware Abstraction Layer
- Schnittstellen zum Hardwarezugriff
- Beispielsweise Festplatten
  - Alle HDDs sind auf die gleiche Art zugreifbar
  - Unabhängig von physikalischem Aufbau
- Ist Teil vom Kernel
- In NTOSKRNL.EXE enthalten



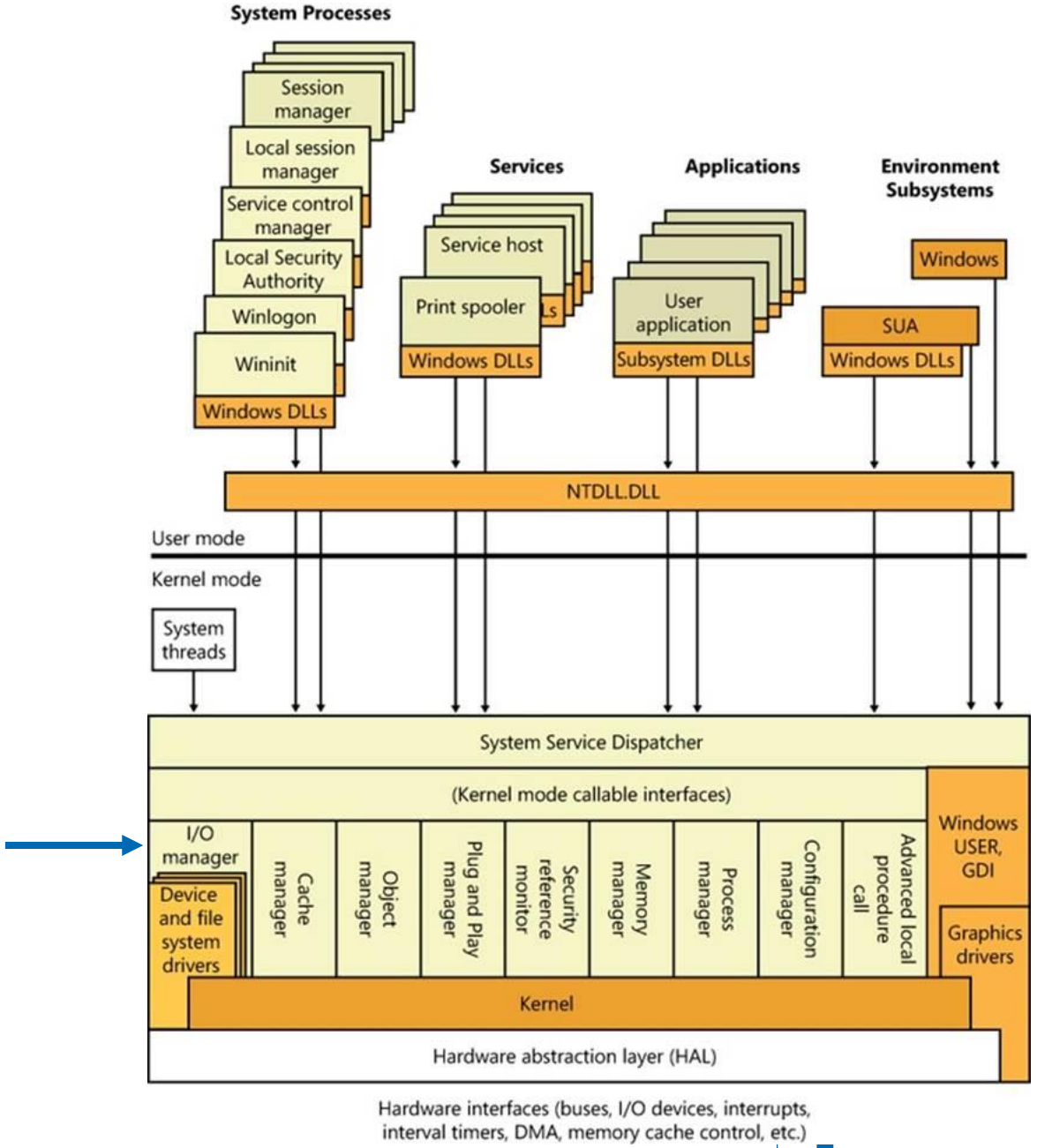
Kernel

- Kern des Betriebssystems
- Verwaltung von Ressourcen, Prozessen und Hardwareinteraktion
- Hybrider Kernel
  - Selbstmanagement (Window Manager)
  - Fremdmanagement (Inter Process Communication (IPC) Manager, Client/Server Subsystem)
- Orientiert sich am Mach Microkernel
- Sicherheitsfeatures zum Schutz vor schädlichen Aktivitäten
- Stellt Systemdienste und Schnittstellen bereit



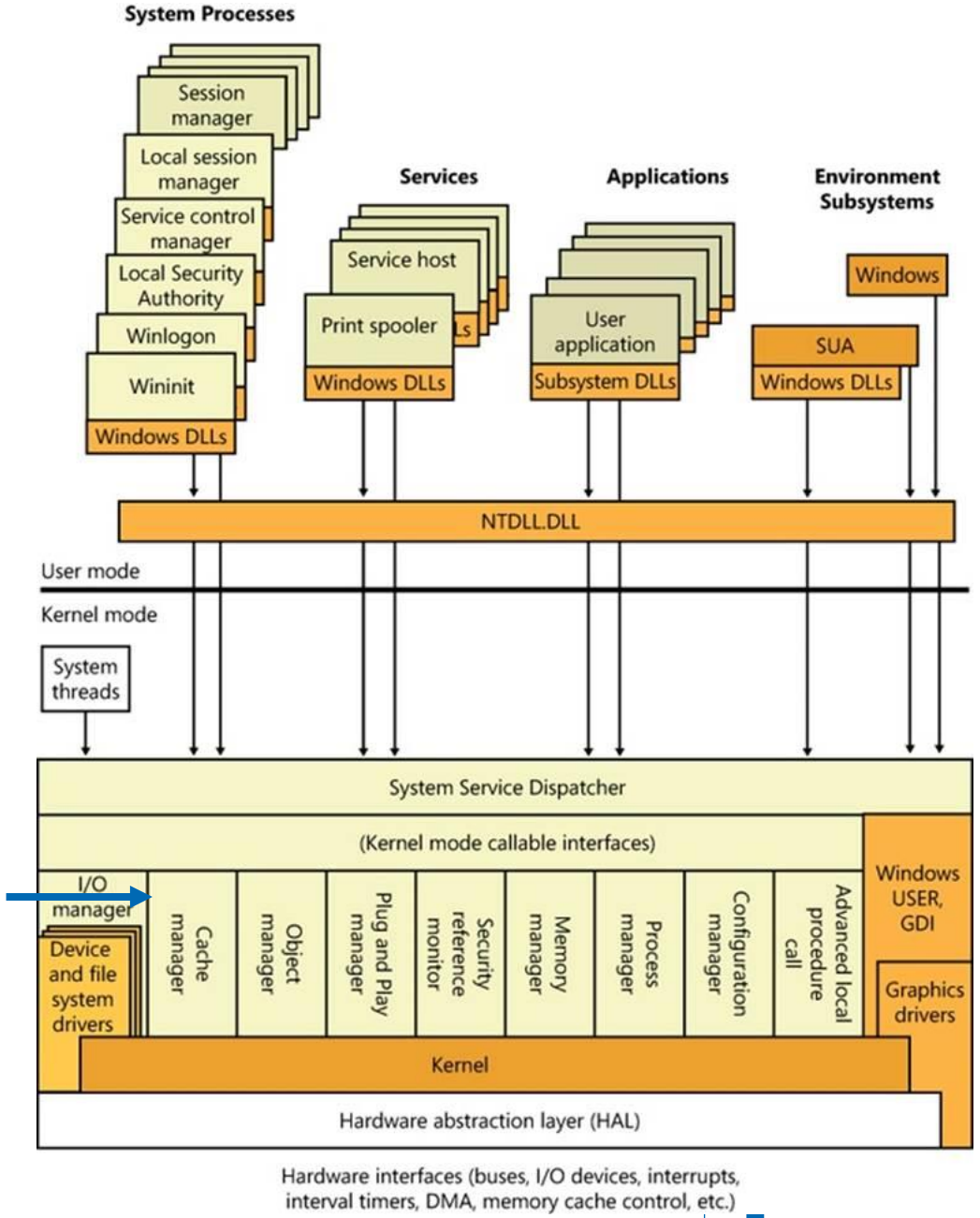
I/O Manager

- Kommunikation zwischen Subsystemen
- Übersetzung von User-Mode read/write in I/O Request Packets
- Aufgaben:
  - Schreiben und Lesen von Daten
  - Koordinieren von Zugriffen auf E/A-Geräte, Dateisysteme und andere Ressourcen
  - Stellt effiziente Ausführung von E/A-Operationen sicher



Cache Manager

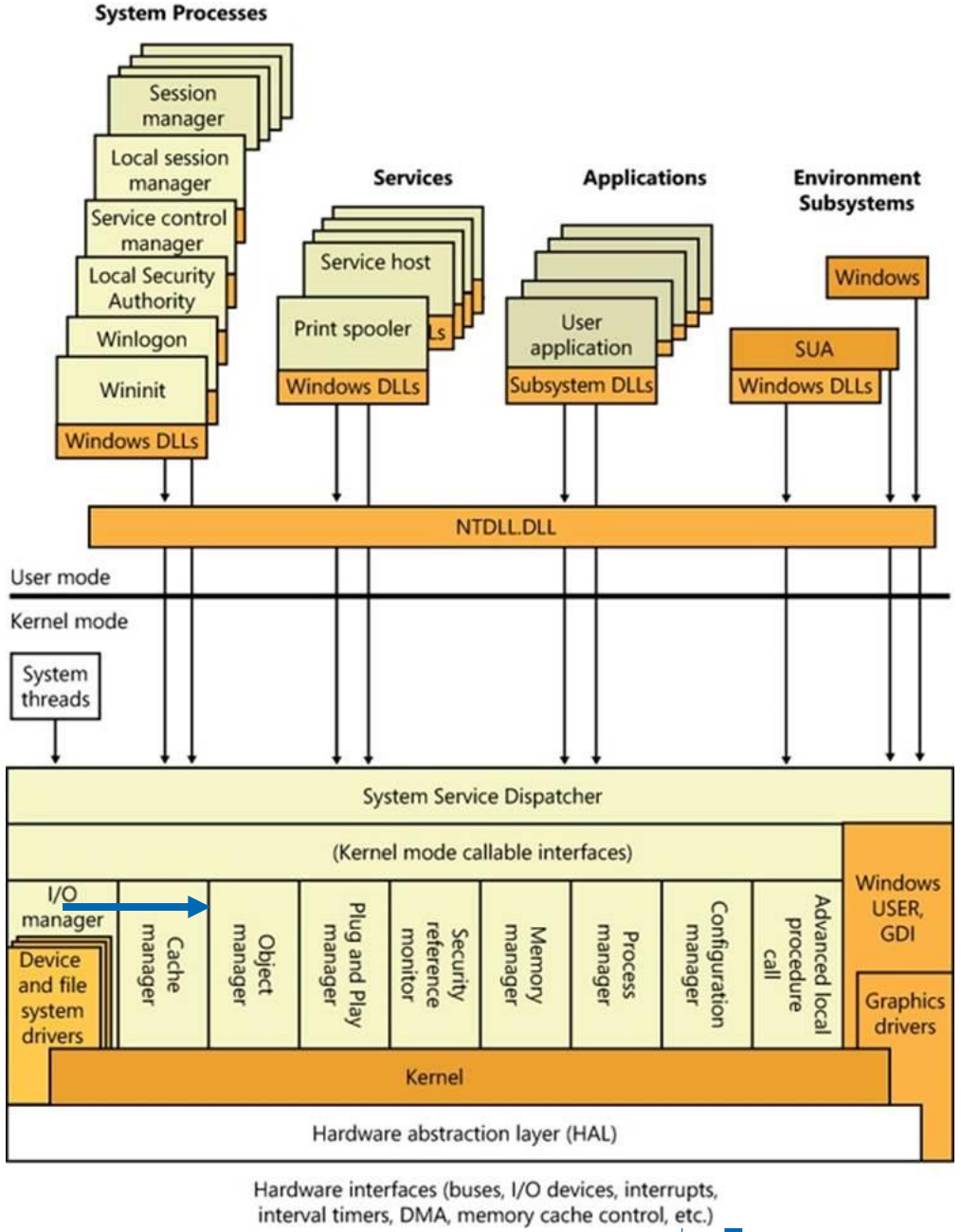
- Arbeitet mit zusammen
  - Memory Manager
  - I/O Manager
  - I/O Drivers
- Cachen von I/O Daten von langsamen Datenträgern
- Arbeitet mit File Blocks
- Zur Beschleunigung wiederholender Speicherzugriffe



Object Manager

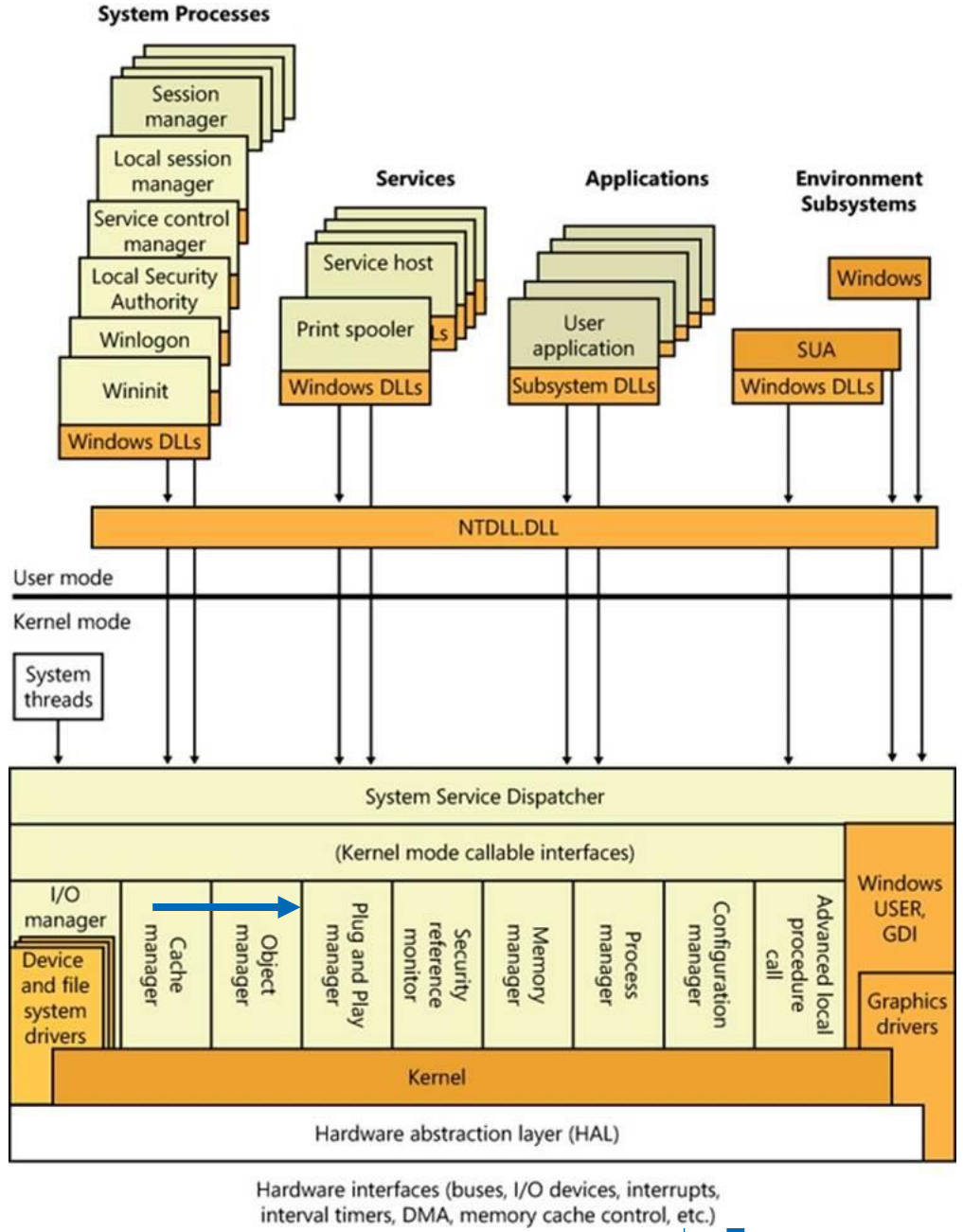
- Gateway für Subsysteme
- Verwaltet Ressourcen Zugang
  - Physikalische Ressourcen
  - Logische Ressourcen
- Sieht alles als Objekte:
  - Dateien
  - Prozesse
  - Threads
  - Registryschlüssel

➢ Windows NT ist Objekt-Orientiertes-Betriebssystem



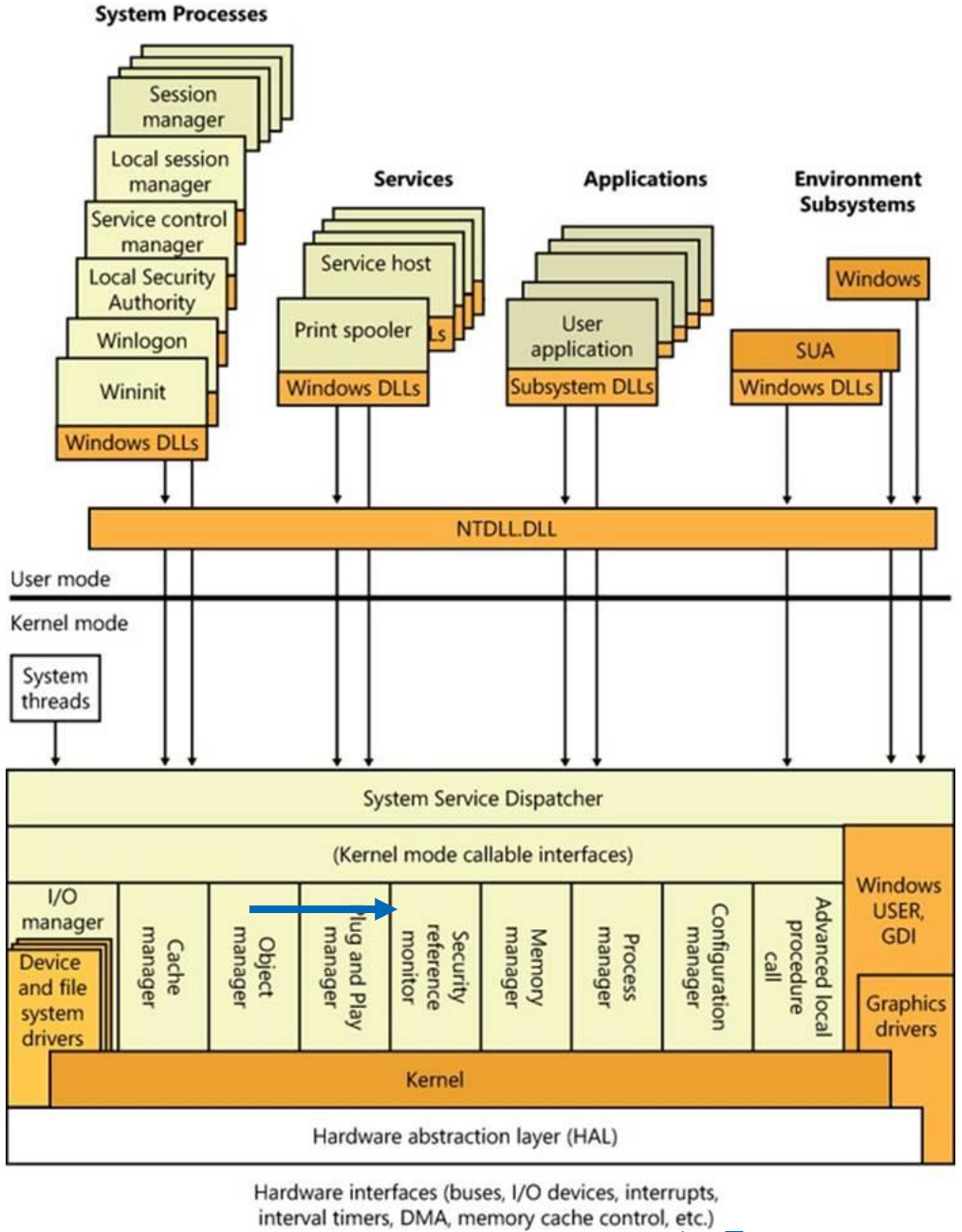
Plug and Play Manager

- Plug and Play Support für
  - Festplatte
  - Game-Controller
  - Audio-Device
  - Netzwerkkabel
  - ...
- Erkennt neue Geräte und installiert automatisch passende Treiber
- Zugriff einrichten/beenden



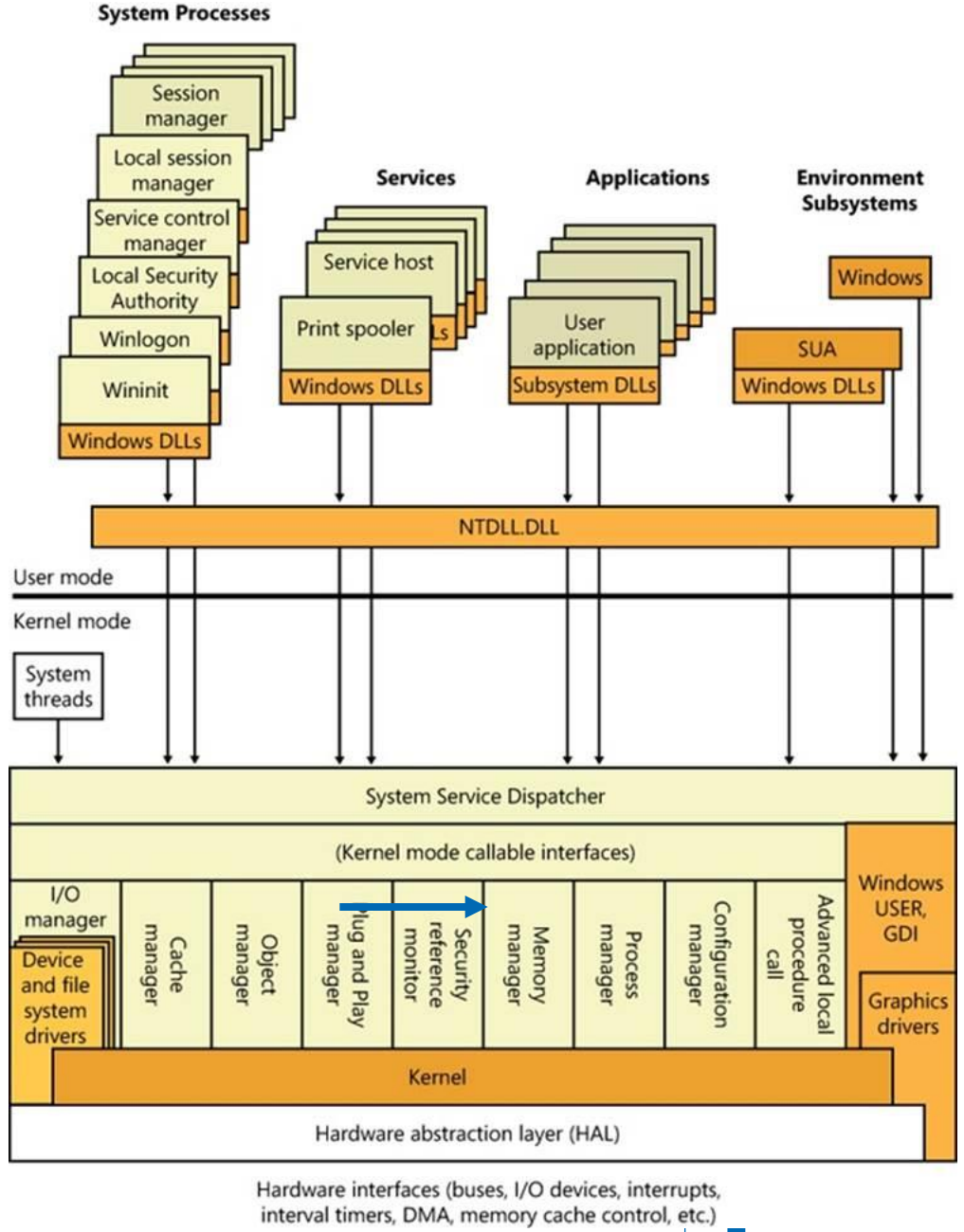
Security Reference Monitor

- Umsetzen von Sicherheitsrichtlinien
- Bestimmen ob auf Ressourcen zugegriffen werden darf
- Wertet Access Control Listen (ACL) aus



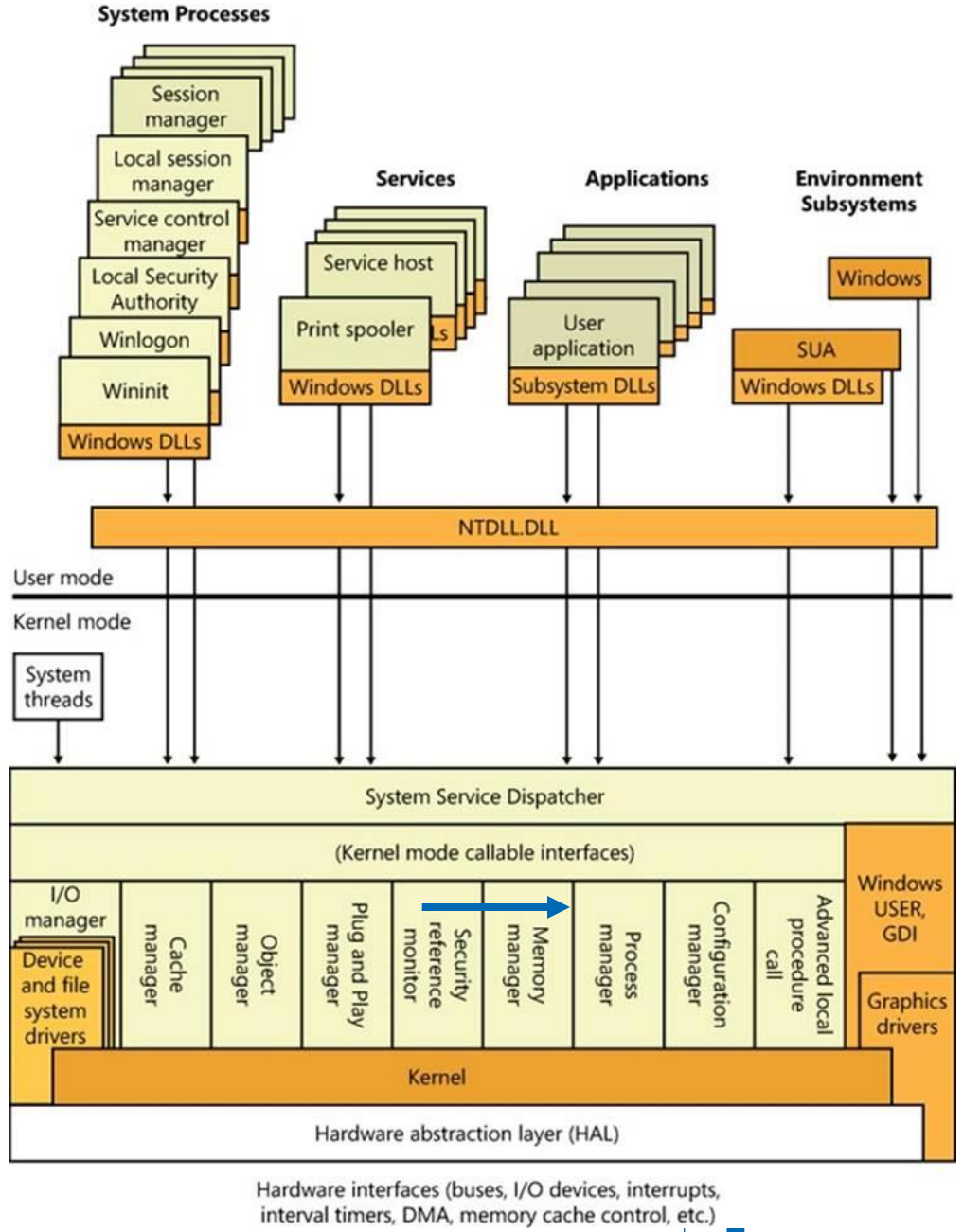
Memory Manager

- Verwaltet physischen und virtuellen Speicher
- Zuständig für
  - Memory Protection
  - Memory Paging
  - General-Purpose Allocator
  - Speicherkomprimierung
  - + Speicherfehlerbehandlung
- Parsen von PE-Executatbles
- Atomares ein- und ausbinden von Anwendungen



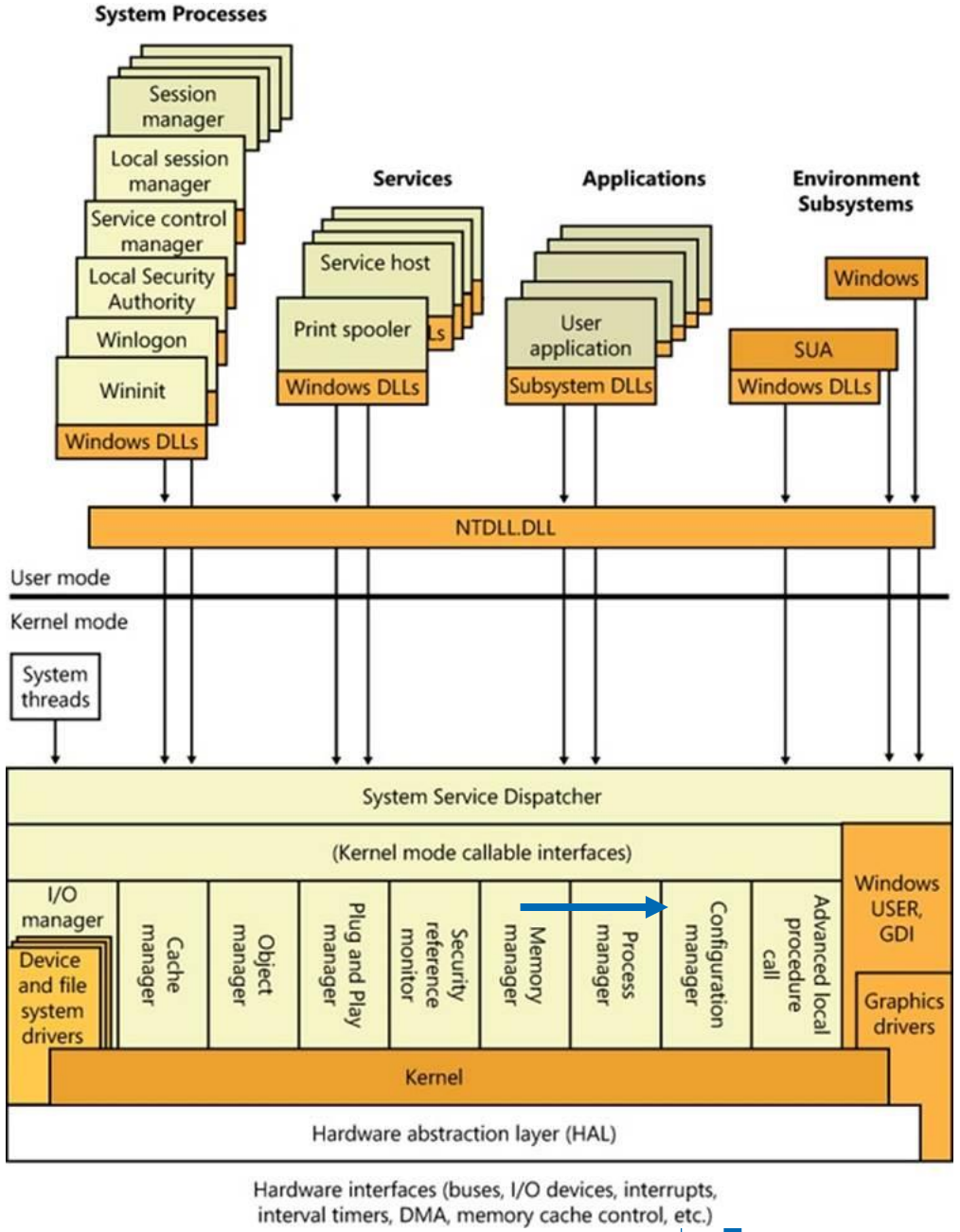
Process Manager

- Verwaltet
  - Prozesse
  - Threads
- Ist zuständig für
  - Erstellen
  - Starten
  - Beenden
- Koordination der Prozesse auf dem Prozessor



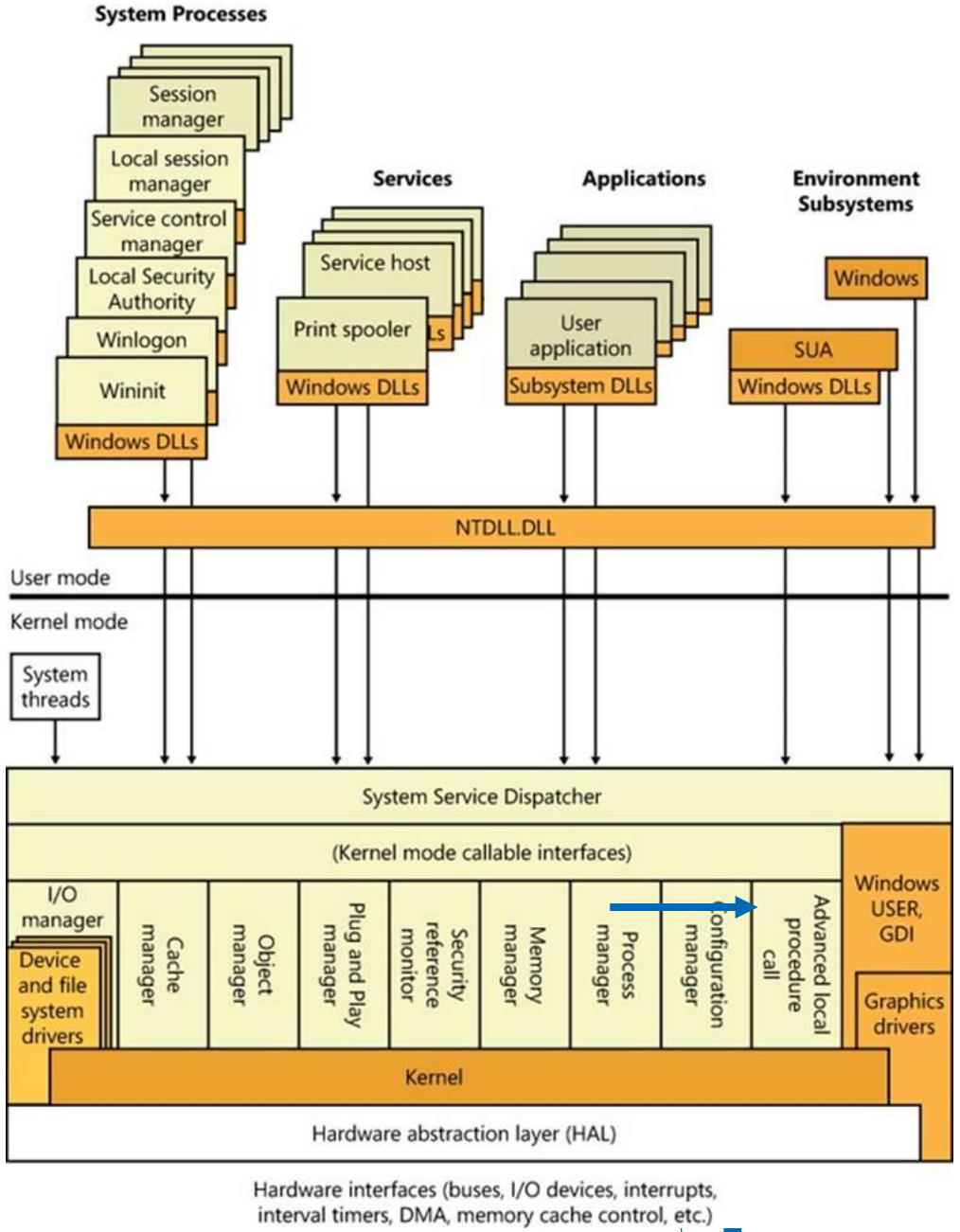
Configuration Manager

- Verwaltet Systemeinstellungen und Konfigurationsdaten
  - Hardware
  - Netzwerk
  - Benutzerkonten
  - Sicherheit
- Hauptanlaufpunkt: Registry
  - Schreiben und Lesen
  - Aktualisierungen der Daten
- Fehlerbehandlung



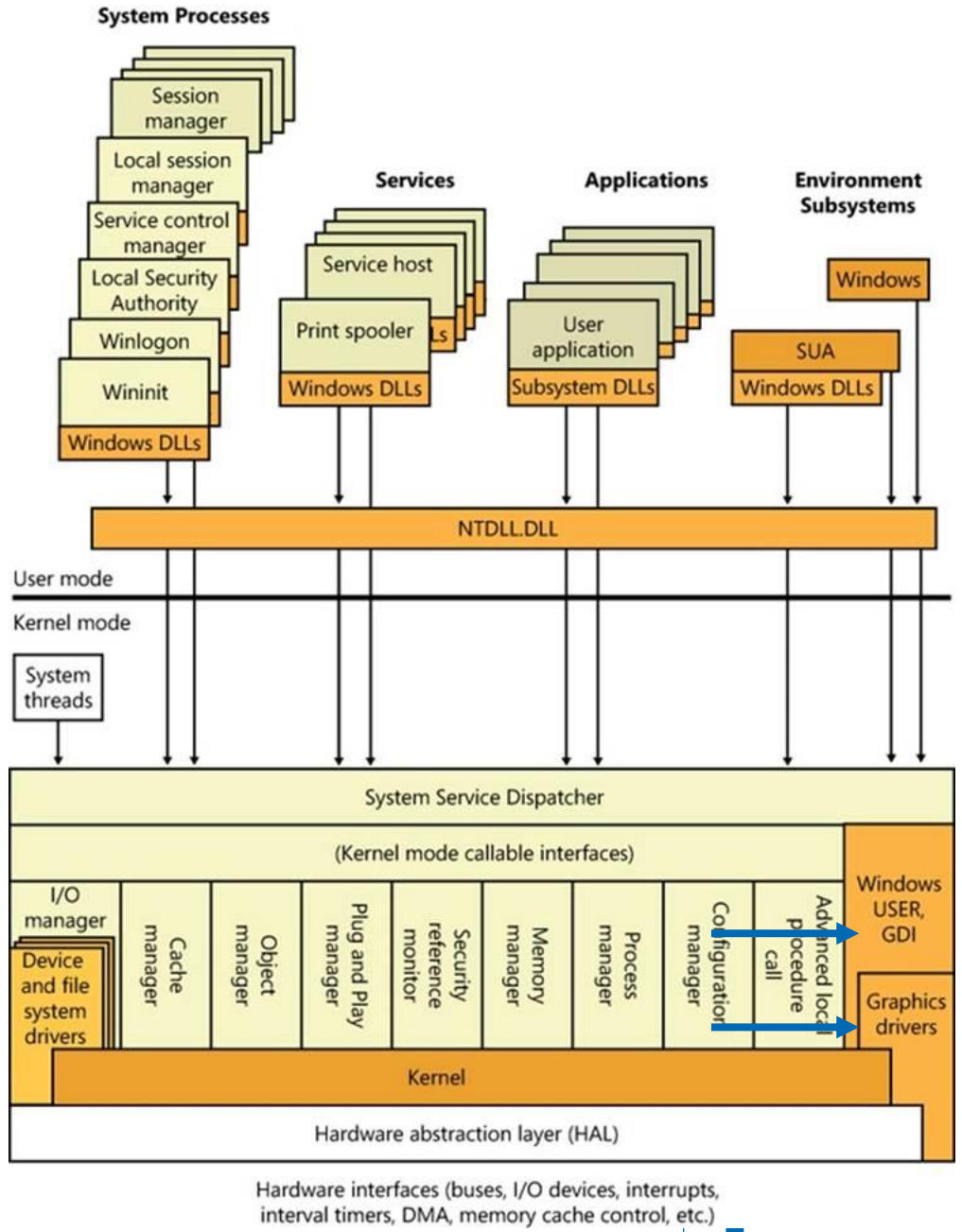
Advanced Local Procedure Call

- Regelt die Inter Process Communication (IPC)
  - Direktes Weiterreichen von Daten per Pointer
  - Zugriffskontrolle zwischen Prozessen
- Informationsleitung zwischen Subsystemen
  - Auswahl des Zielsubsystems
  - Speicher Mapping innerhalb von Subsystemen
- Sehr hohe Skalierbarkeit → auf eine Vielzahl an Prozessen anwendbar



Graphics Drivers / Windows User GDI

- Zeichnen von
  - Linien
  - Pixeln
  - Kurven
  - Kreisen
- Farbverwaltung
- Darstellen von
  - Bildern
  - Fenstern
  - 3D-Objekte

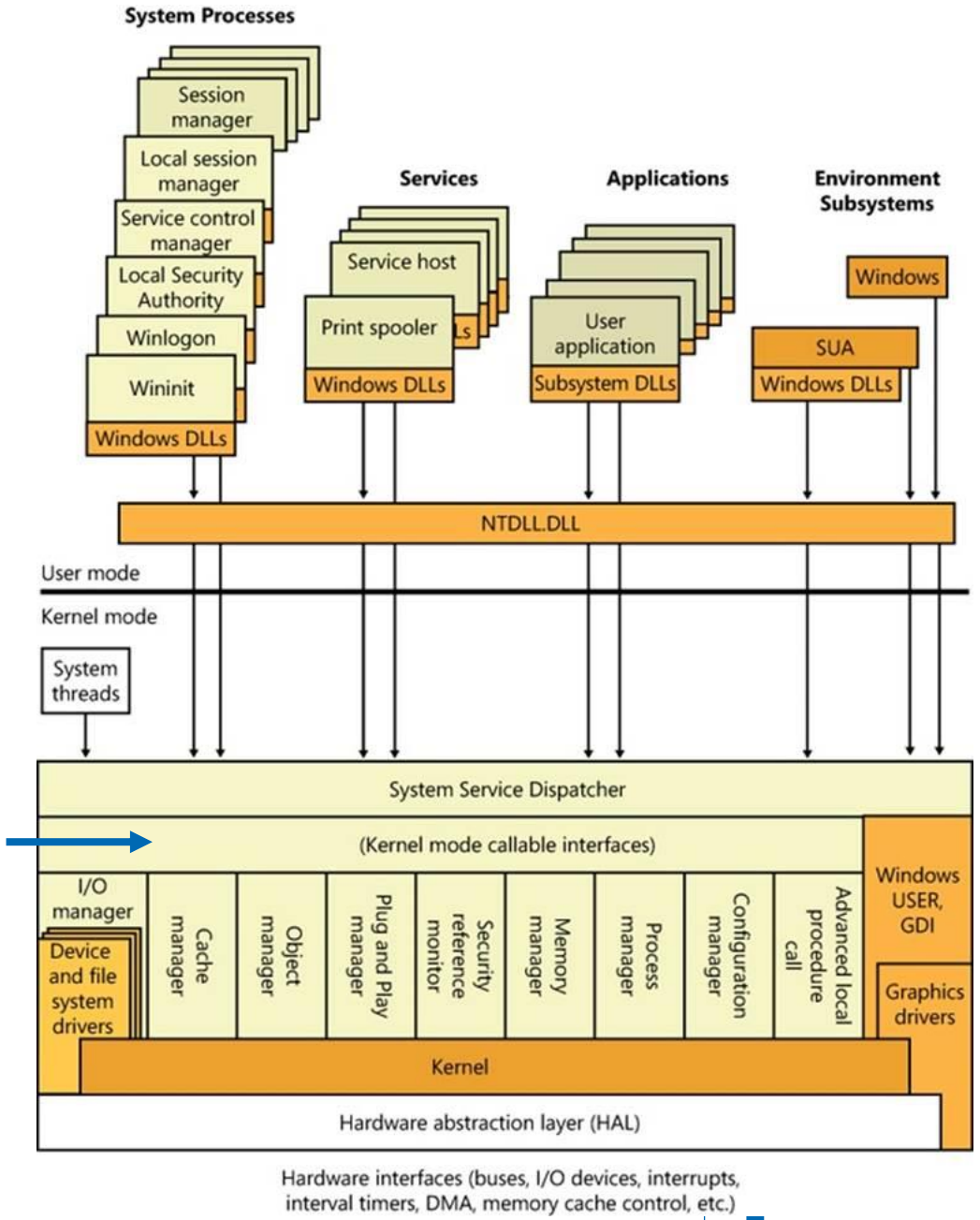


Kernel Mode Callable Interfaces

- Weiterleitungsschicht zwischen Kernel- und User-Mode
  - Stellt Schnittstellen für User-Mode bereit
  - Damit können Benutzeranwendungen auf Kernelressourcen zugreifen

➢ Keine Autorisierung der Zugriffe

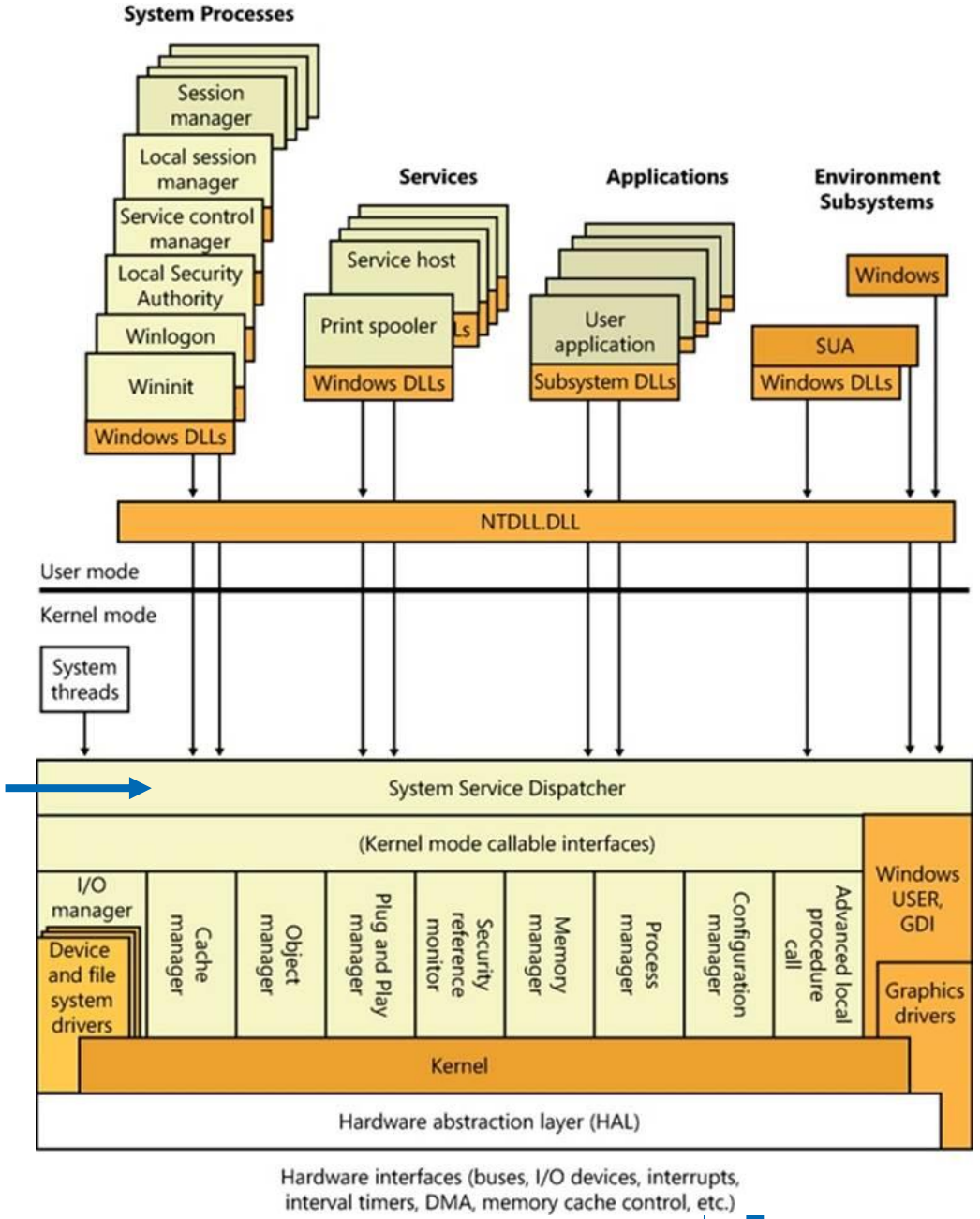
➢ Reine Weiterleitung an entsprechendes Modul



System Service Dispatcher

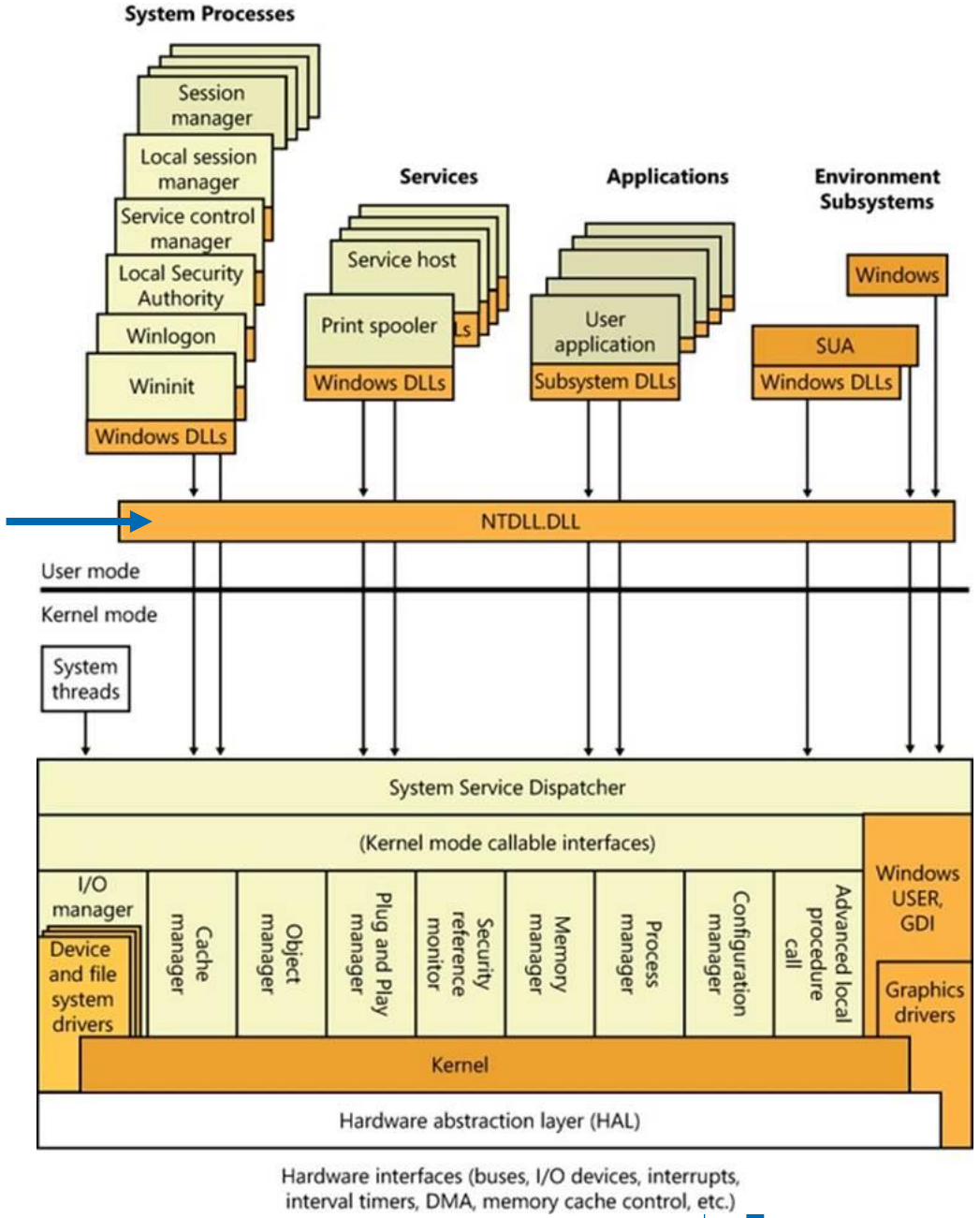
- Sicherheitsüberprüfung der Systemaufrufe an Kernelkomponenten
- Validierung und Weiterleitung der Anfragen an KMCI
- Mechanismen für:
  - Fehlerbehandlung
  - Sicherheit

➢ Ziel: Schutz der Integrität und Stabilität des Systems



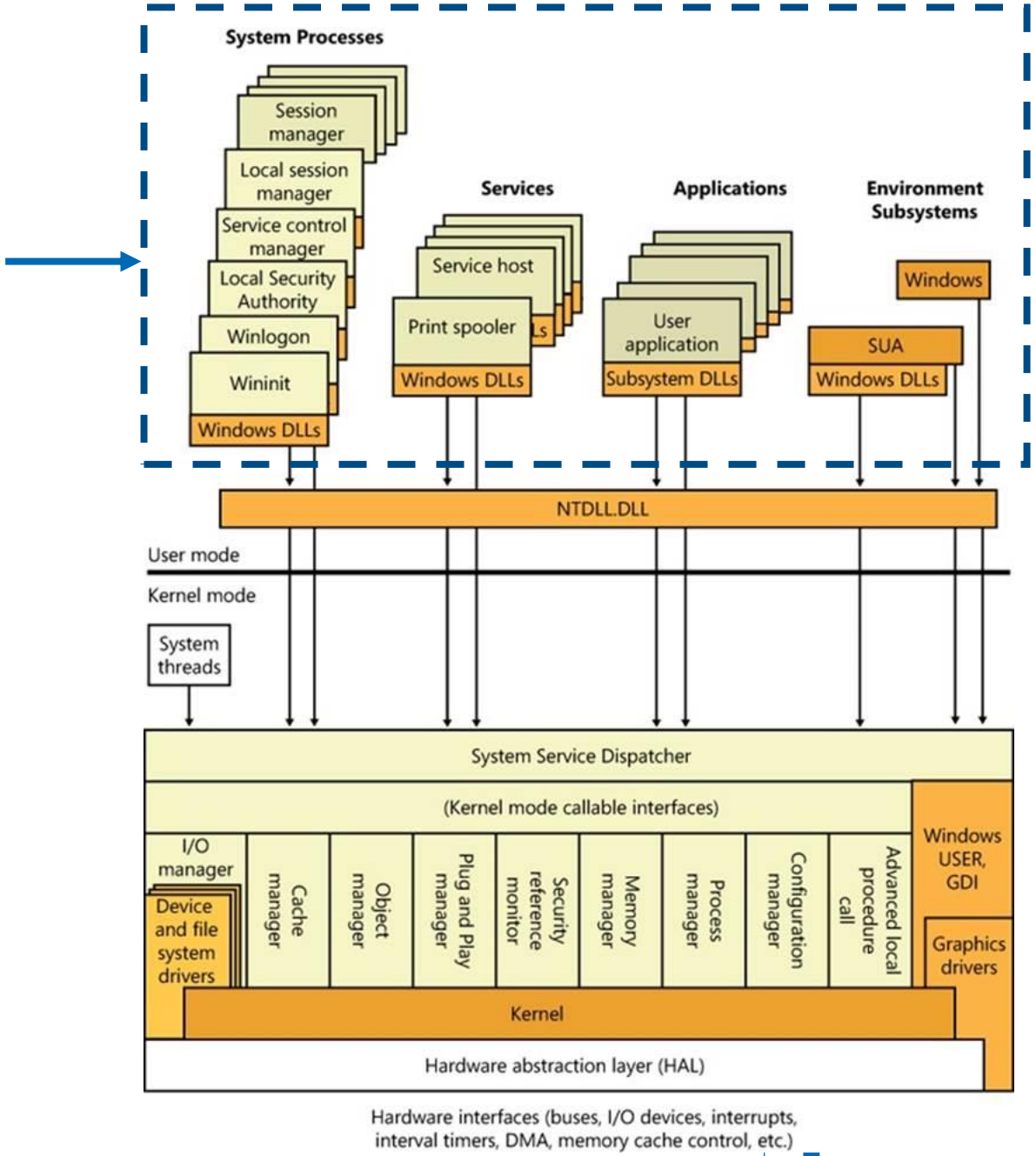
NTDLL.DLL

- Schnittstelle für User-Prozesse
- Hauptsächlich Mapping von Kernel-APIs in User-Space
- Enthält alle aufrufbaren Funktionen des Kernel-Spaces und stellt sie als Bibliothek um User-Space bereit
- Anhand der Funktionen können Aufrufe an die SSD generiert werden



Anwendungen

- Systemanwendungen
  - Anmeldemanager
  - Druckerwarteschlange
  - Datei-Explorer
  - …
- Benutzeranwendungen
  - Power-Point
  - Gimp2
  - …
- Subsysteme
  - Ubuntu
  - Android
  - …



Zusammenfassung

Zusammenfassung

Heute haben Sie die Historie und den Entwicklungsprozess des Microsoft Windows Betriebssystems erfahren.

Es wurde auf die einzelnen Betriebssystem Versionen und für Windows 10 auf die unterschiedlichen Lizenz-Editionen eingegangen. Damit sollte grob bekannt sein, welche Features mit welcher Version implementiert wurden. Darüber hinaus sollte die Vermarktungsstrategie von Microsoft der letzten Jahre deutlich geworden sein.

Zuletzt haben Sie die Windows-NT Architektur kennen gelernt. Hierbei wurde auf die einzelnen Komponenten eingegangen. Es wurde ein kurzer Überblick über deren Funktion gegeben.

Vielen Dank

Tim Wetterau B.Sc.

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Angewandte Computer- und Biowissenschaften

T +49 (0) 3727 58-1752
@ wetterau@hs-mittweida.de
www.cb.hs-mittweida.de

Haus 8 | Richard-Stücklen Bau| Raum 8-303
Am Schwanenteich 6b| 09648 Mittweida

HOCHSCHULE MITTWEIDA
University of Applied Sciences

hs-mittweida.de