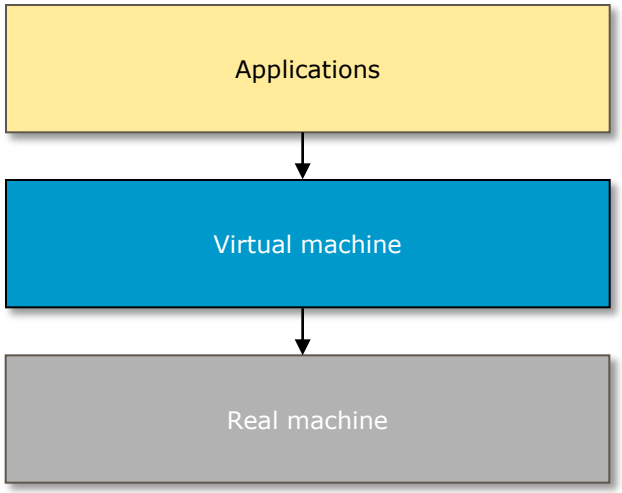
# Essential Windows Kernel Mode Components

## Overview

- Organization
- Model
- Components
- CPU Modes
- System processes
- Services processes
- Users processes
- Subsystems processes
- System services

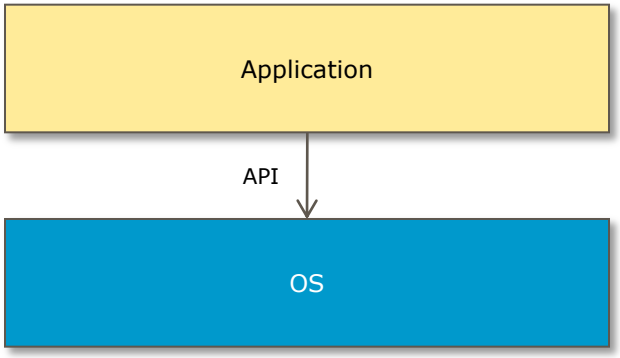
# OS Organization

- Access to hardware is not allowed
- Access to hardware is made via system services

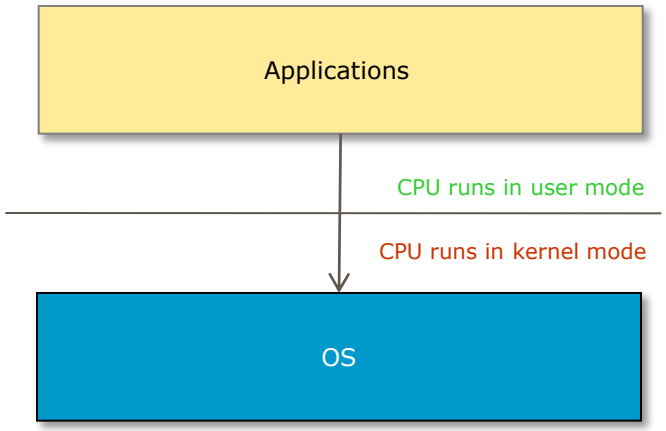


# OS Model

- Applications access the OS via one defined Application Program Interface (API)

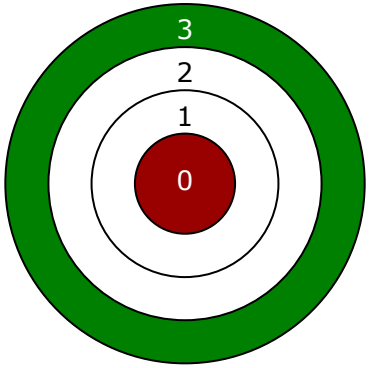


# OS Contexts


Applications
CPU runs in user mode
CPU runs in kernel mode
OS

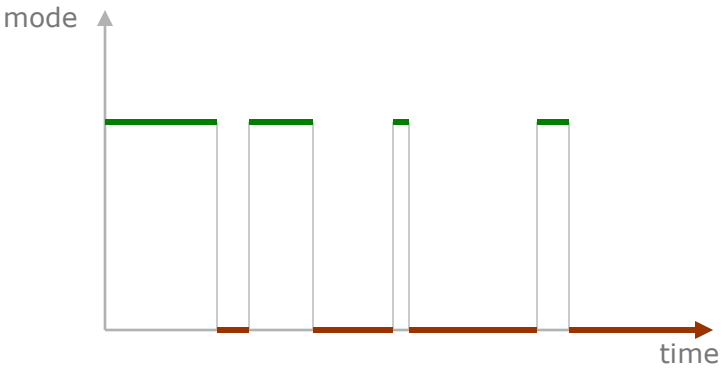
## CPU Modes

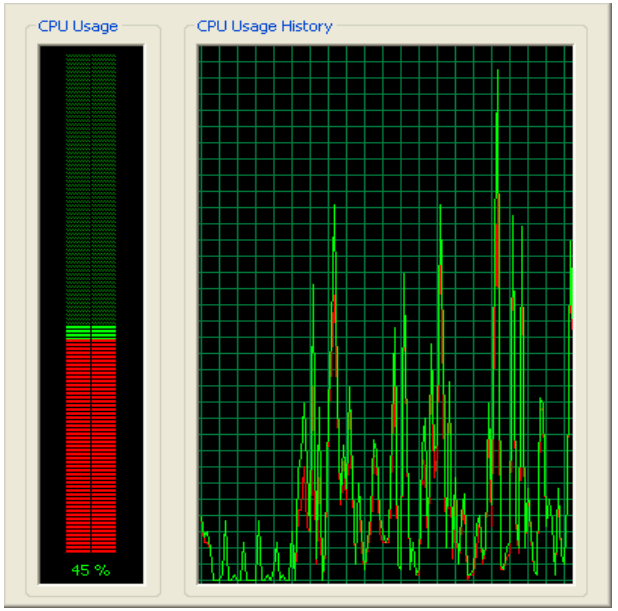
- Protect critical system data from user applications
  - User mode
  - Kernel mode



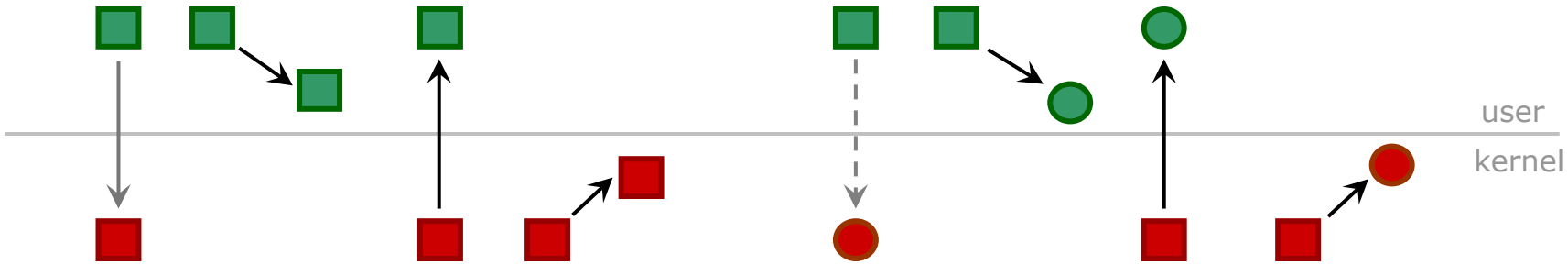
# CPU Modes - mechanism

- User programs typically run in both modes
- CPU mode switch <> CPU context switch



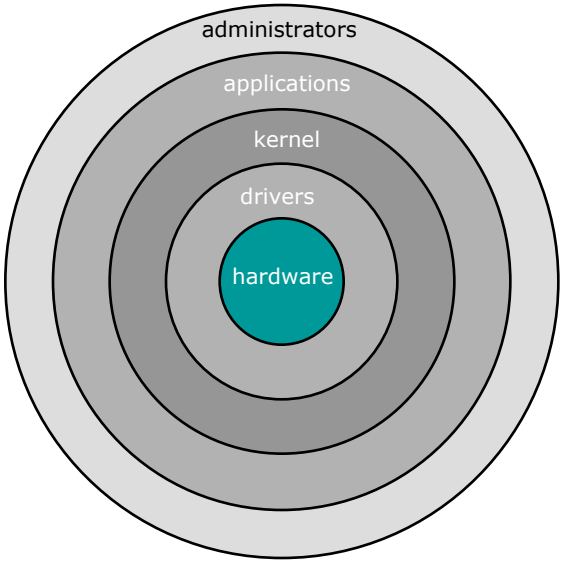
## CPU Modes - scenarios



# Essential Windows Kernel Mode Components

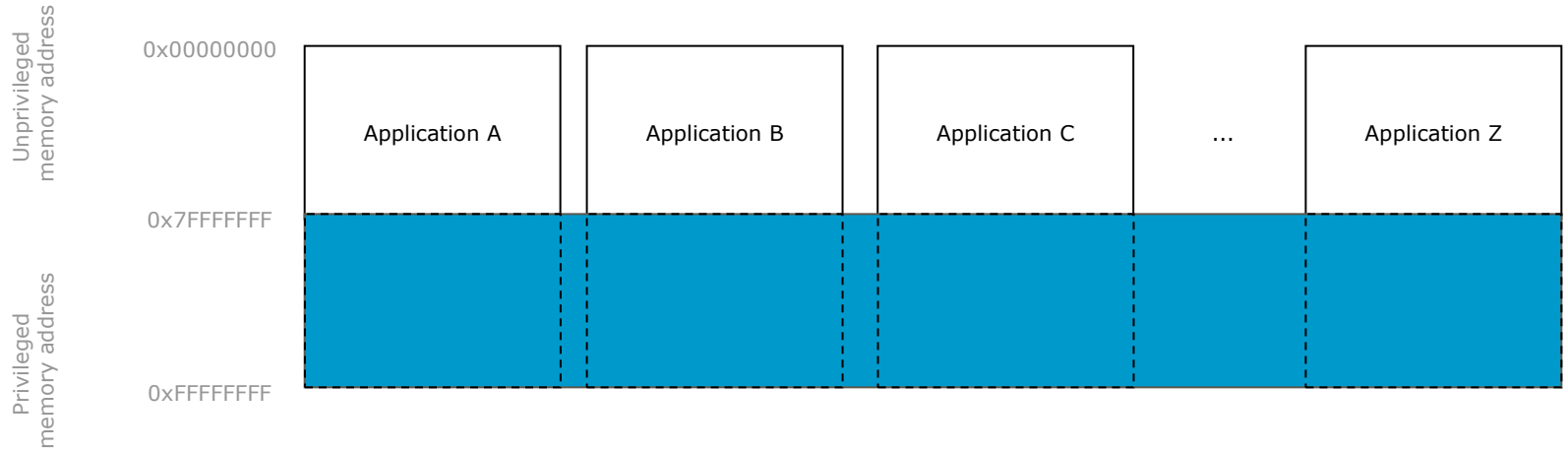
## TCB

- Context
  - No CPU restriction in kernel
  - No memory restriction in kernel
  - No security check in kernel
- Definition
  - Portions of the system trusted to enforce the security
- Components
  - Most hardware
  - All kernel code
  - Some user code (SeTcbPrivilege)
  - Administrators



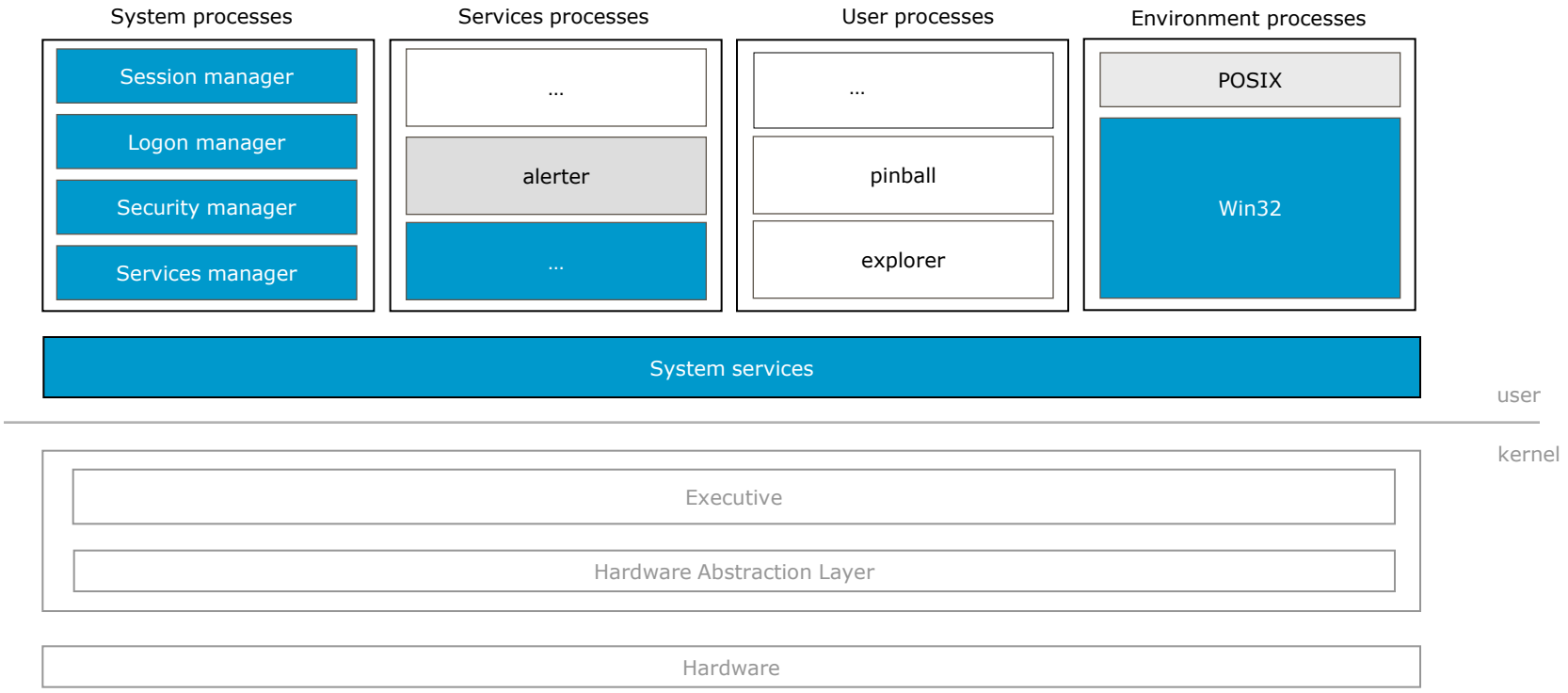
# Memory Layout

- Each application occupies 4 GB of address space
- All applications share system memory space



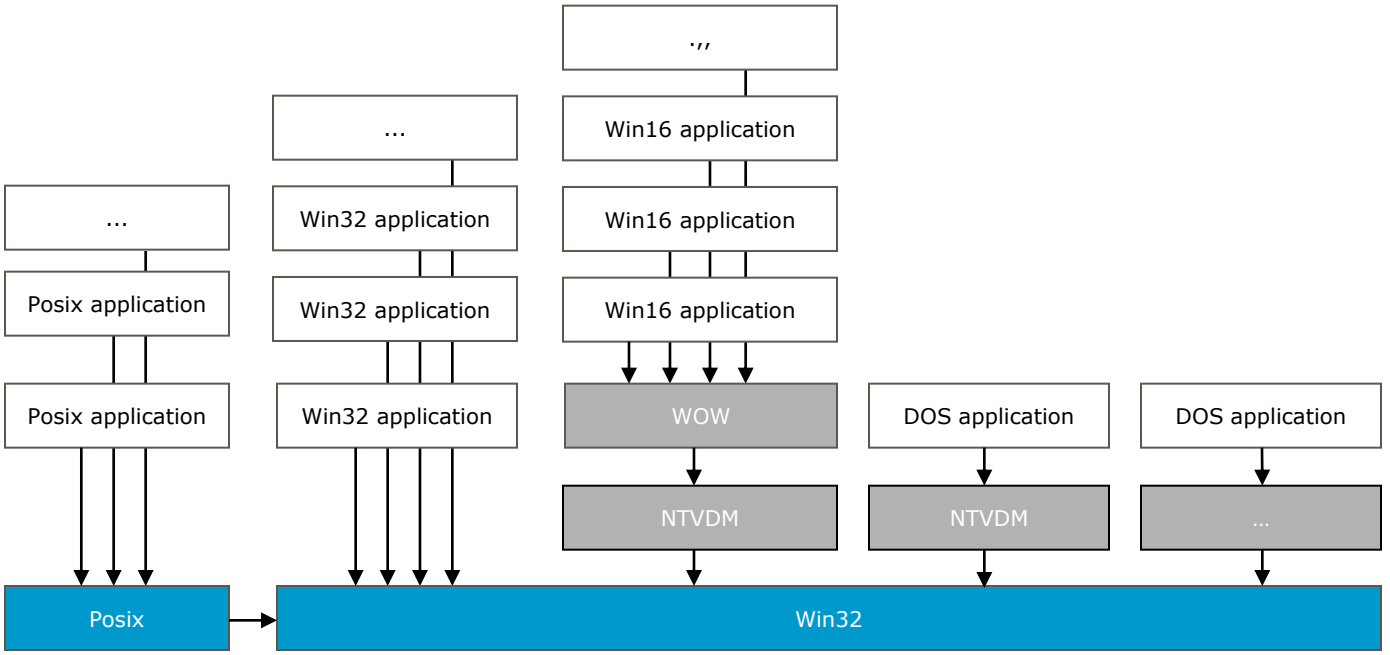
# Essential Windows Kernel Mode Components

## OS Major Components



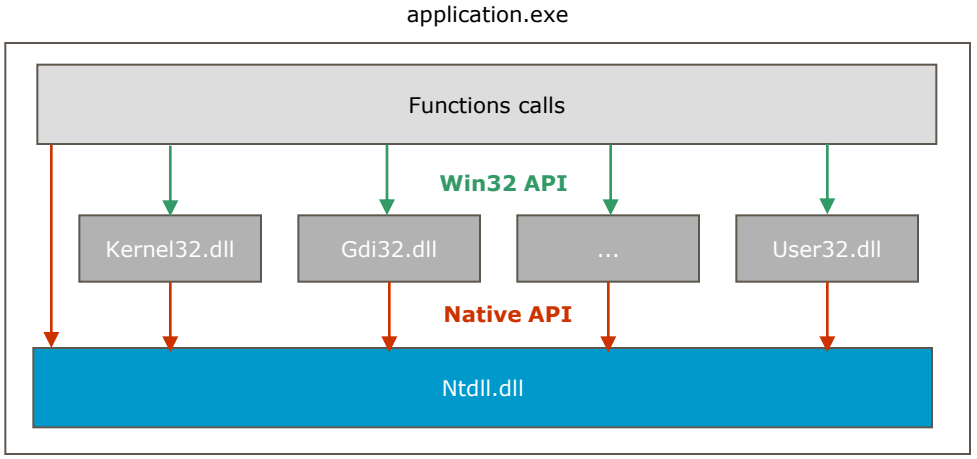
# Environment Subsystems

- Definition
- Role
- Types

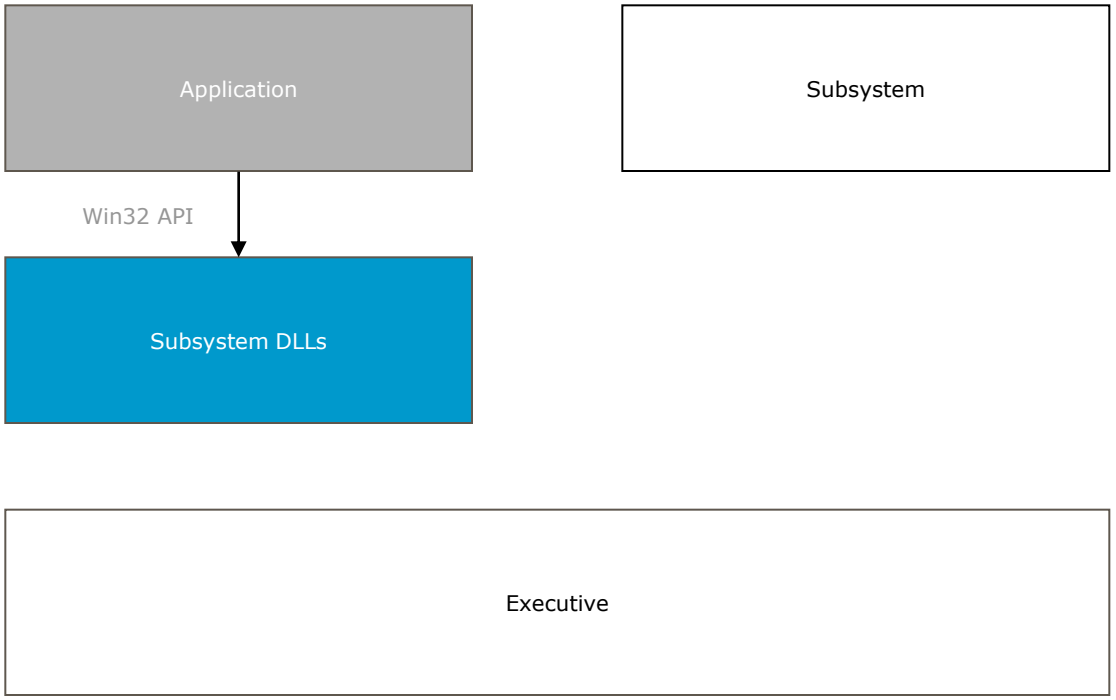


# Environment Subsystems - interfaces

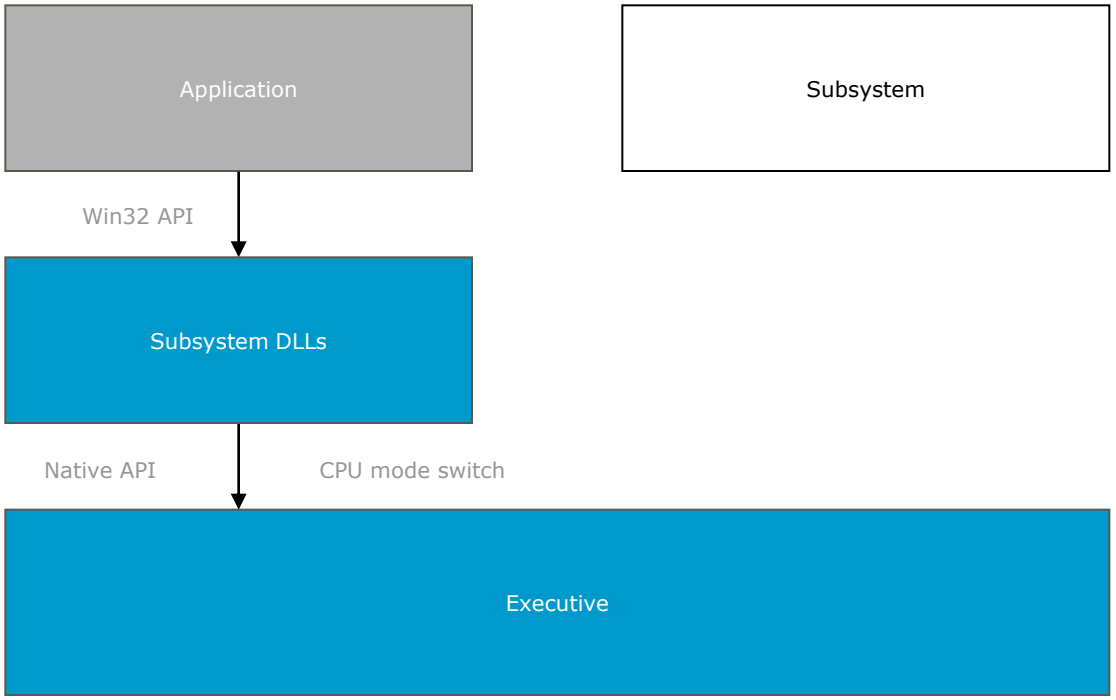
- Subsystem
  - Process runs in a private address space
- Application
  - Sends messages to subsystem
  - Unaware of messages
  - Implicitely linked with systems‘s interfaces (image = code + metadata)



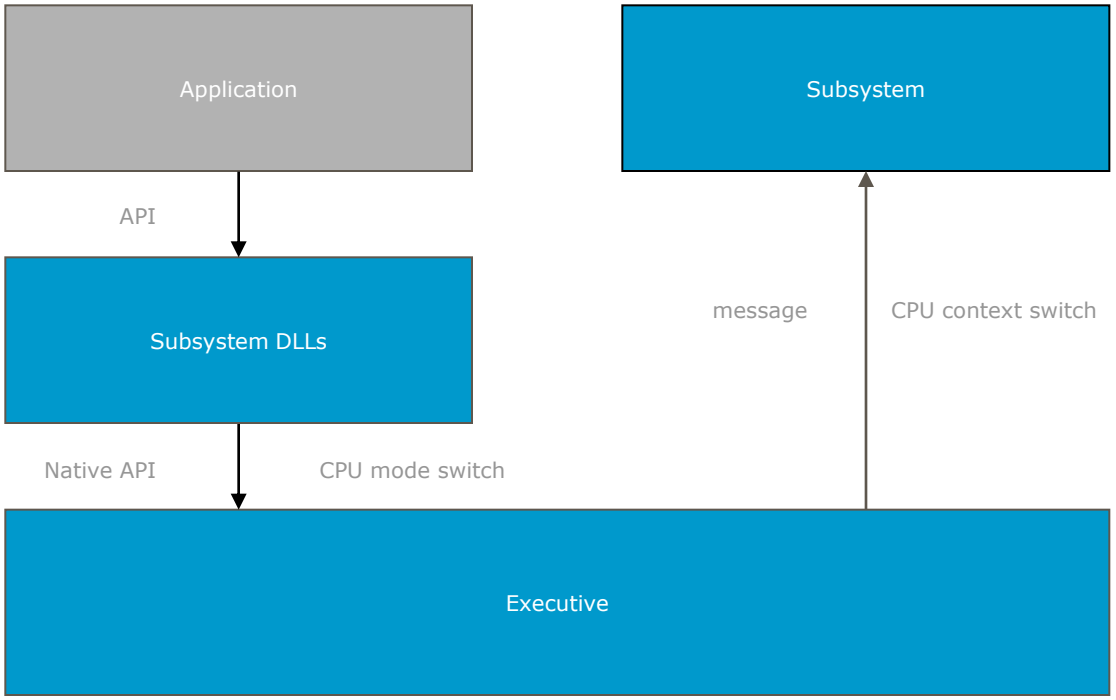
# Environment Subsystems - strategy



# Environment Subsystems - strategy



# Environment Subsystems - strategy

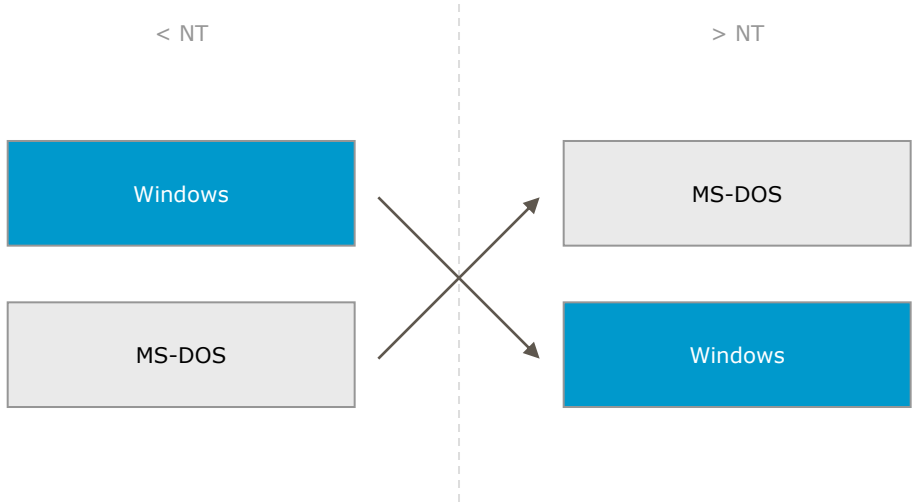


# Environment Subsystems - strategy

| Service implementation | CPU mode switching | CPU context switching | Message sent |
|---|---|---|---|
| User process | No | No | No |
| Executive | Yes | No | No |
| Server | Yes | Yes | Yes |

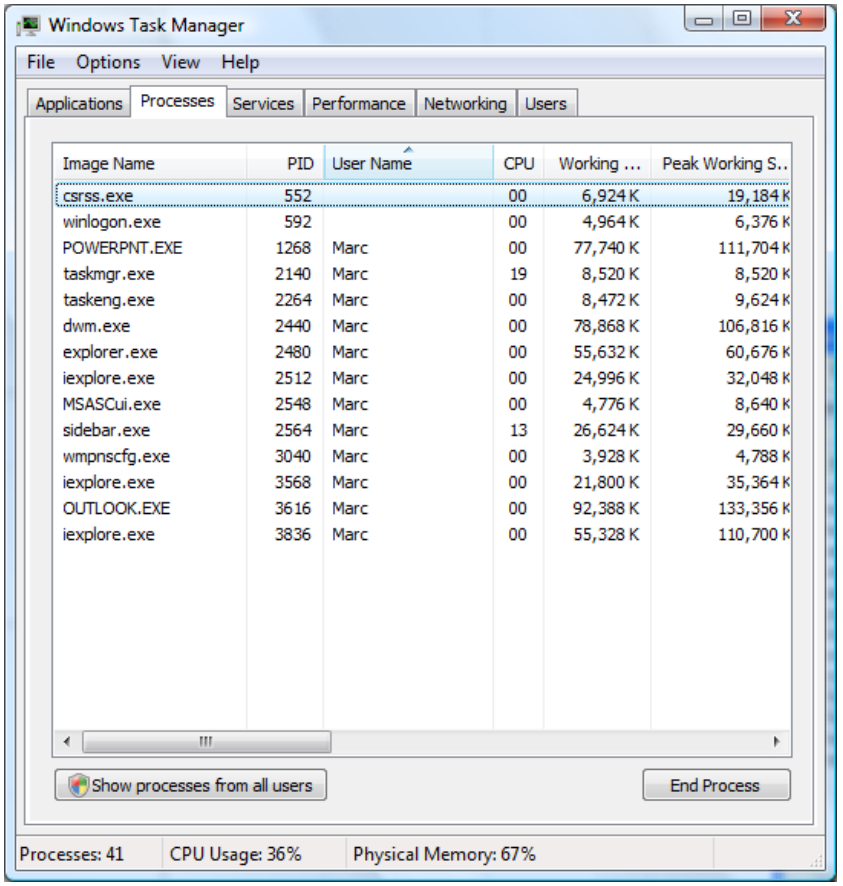
# Win16 Support

- MS-DOS applications
  - One-one relation
- Win16 applications
  - Many-one relation



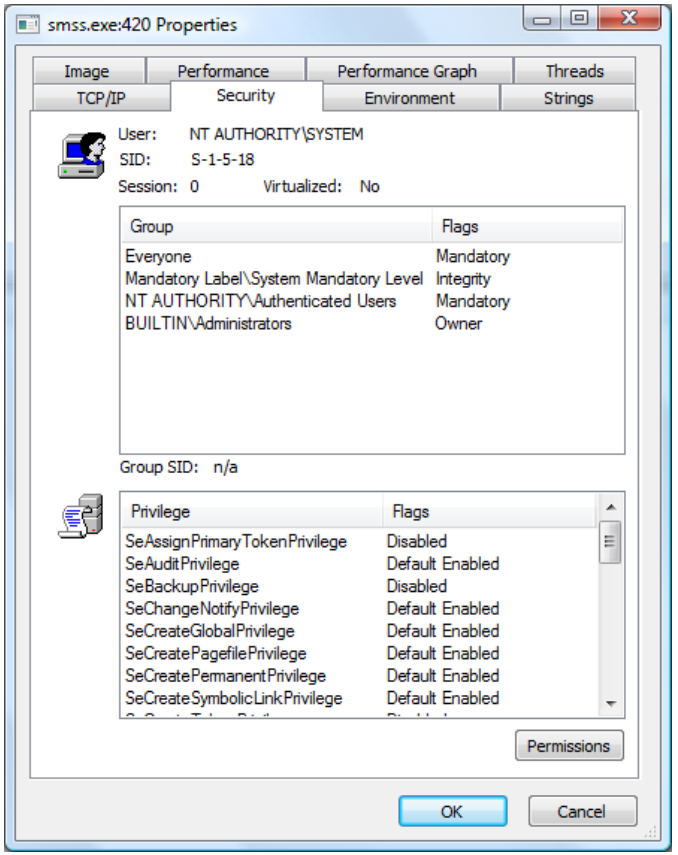
# System processes

- Are started by the system
- Are running on every system
- Cannot be stopped



# Session Manager Subsystem

- Definition
- Role
- Particularities
  - Part of the TCB
  - Native user application



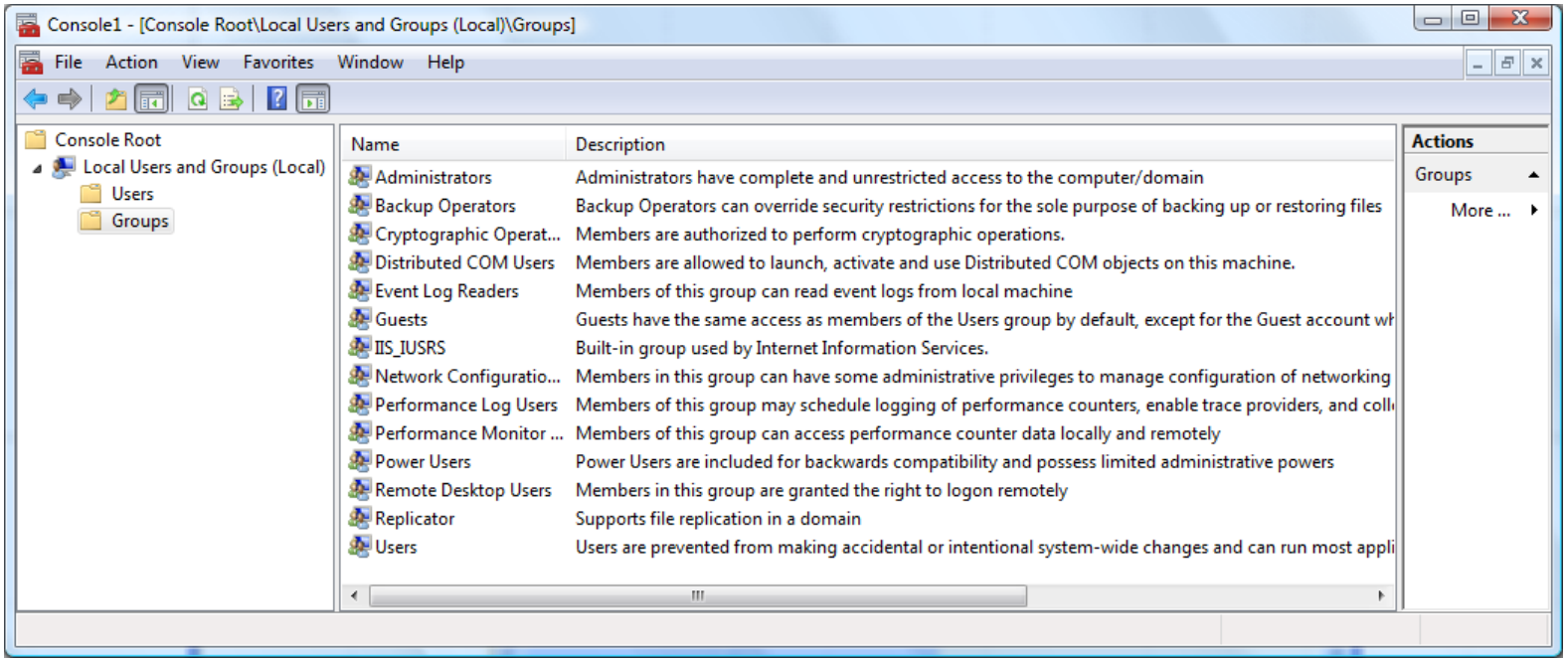
# Logon Manager

- Definition
- Role
  - Interactive logon request management
  - Authentication User interface management
  - User profile initialization
  - Shell creation
  - TASKMGR management

| Who you are (identification) | |
|---|---|
| What you know (authentication) | What you are (authentication) |

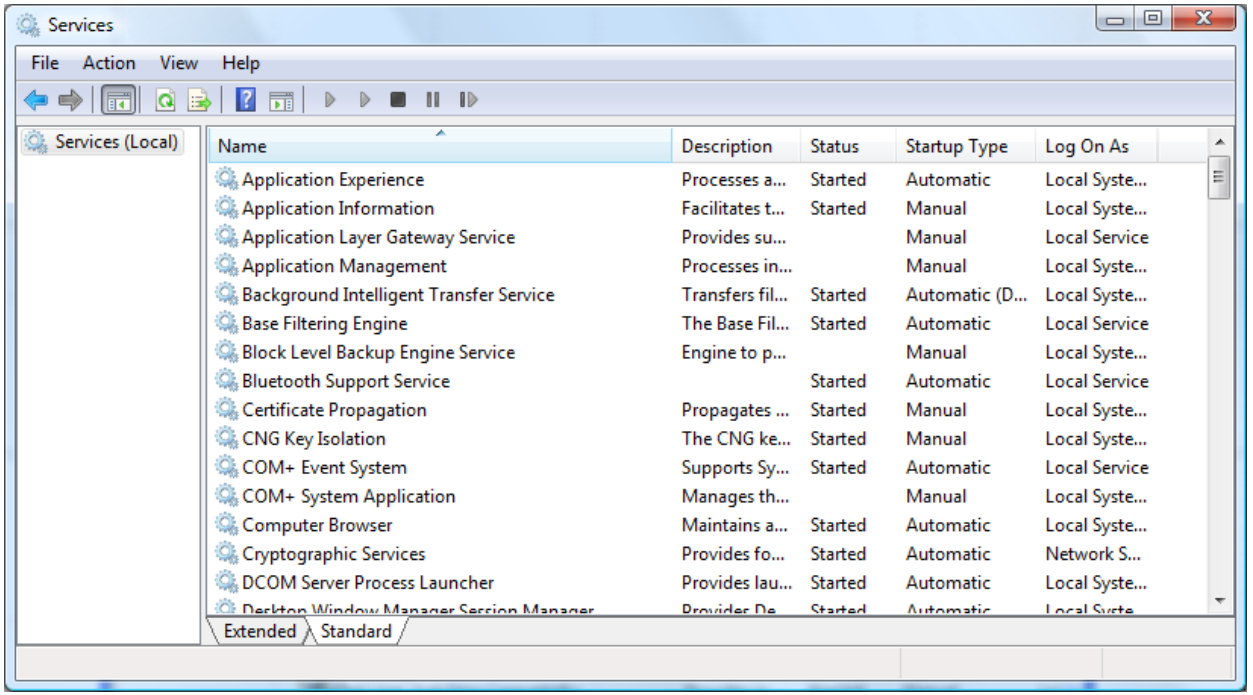
# Local Security Authority Subsystem

- Definition
- Role

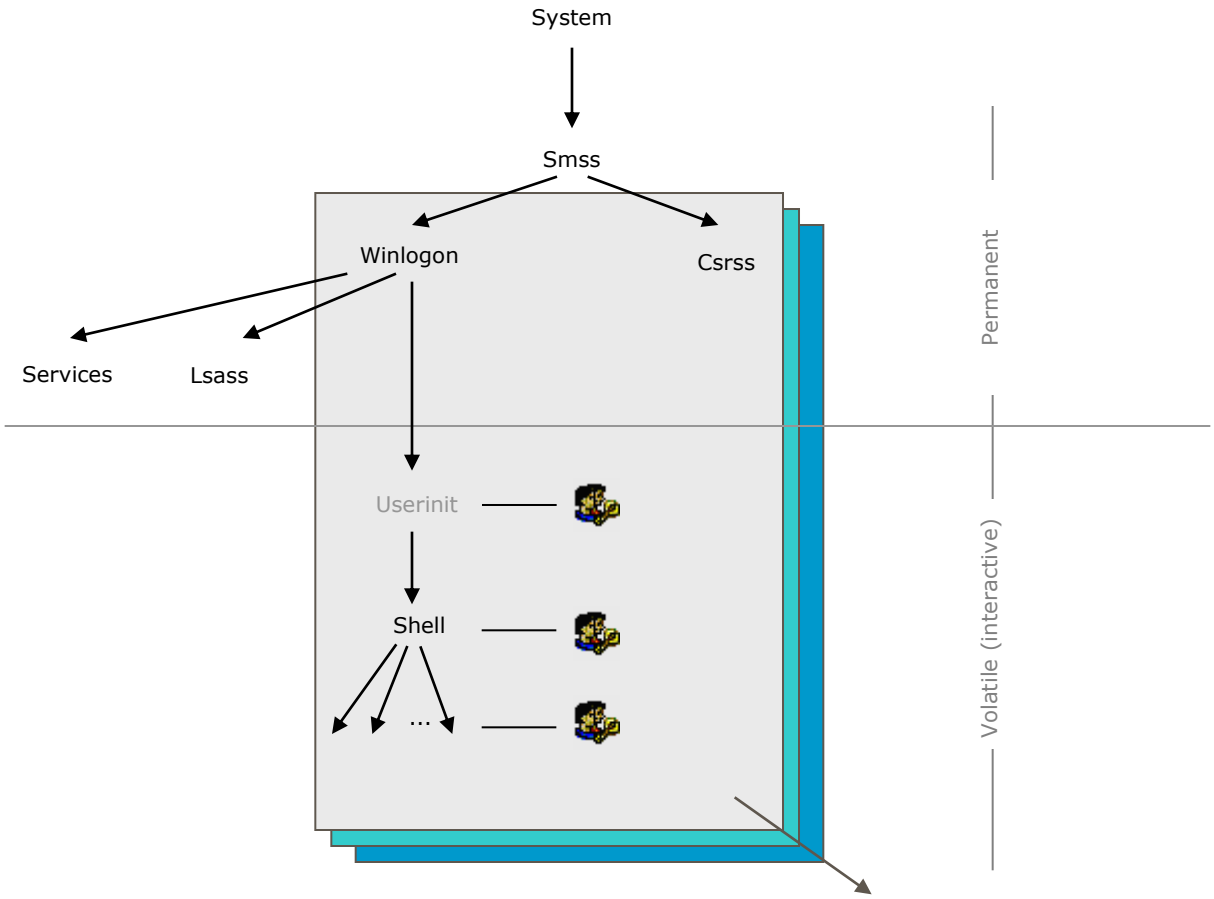


# Service Control Manager

- Definition
- Role



# User Processes - creation



# Essential Windows Kernel Mode Components

Thanks!