Linux Sicherheit

Kerngestützte Sicherheit mit RSBAC

Stefan Berthold

dingx@atlantis.wh2.tu-dresden.de

Linux User Group Dresden

http://lugdd.schlittermann.de/

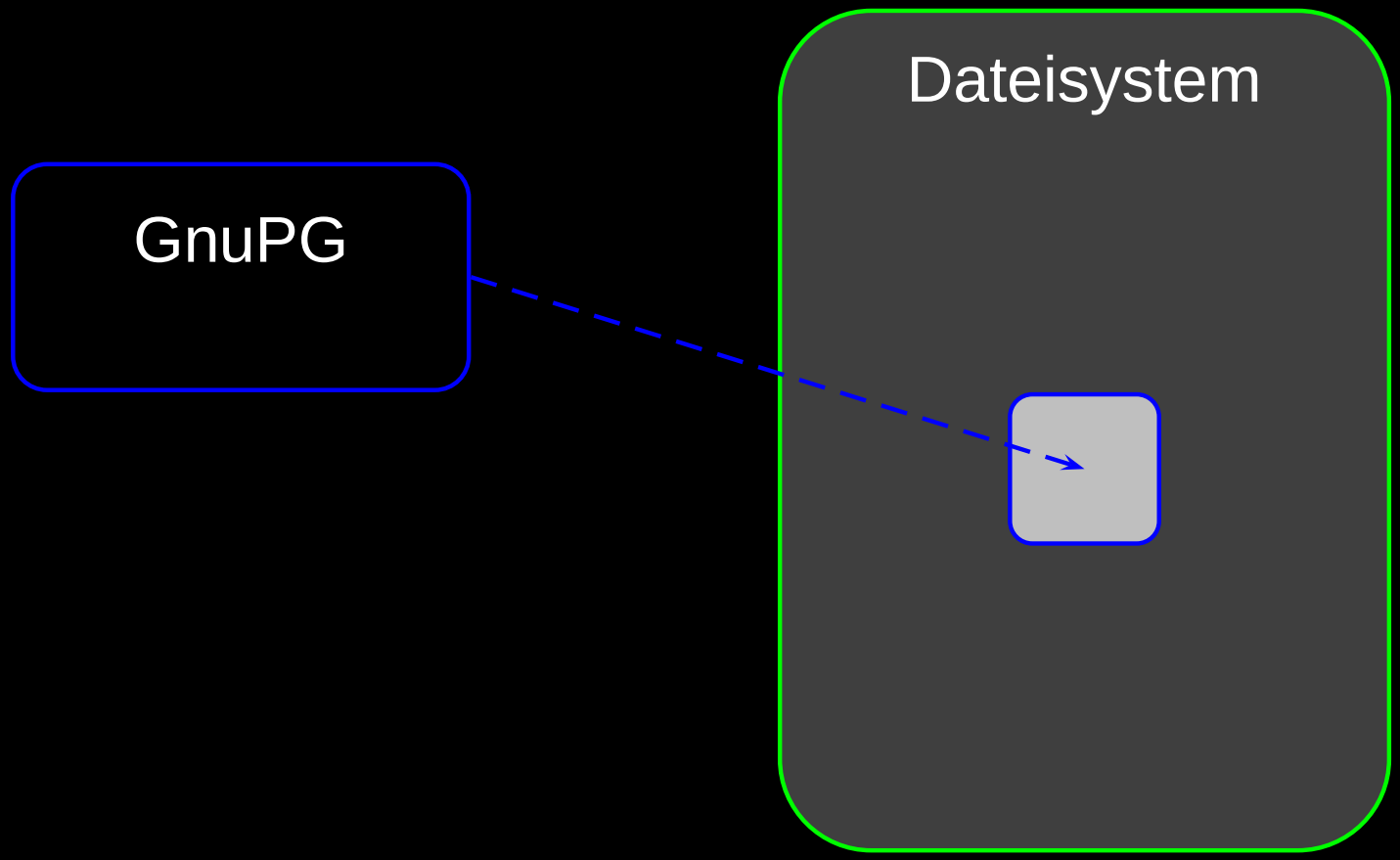
Was soll besprochen werden?

- Einführung von *normalen* Sicherheits-mechanismen in Endsysteme.

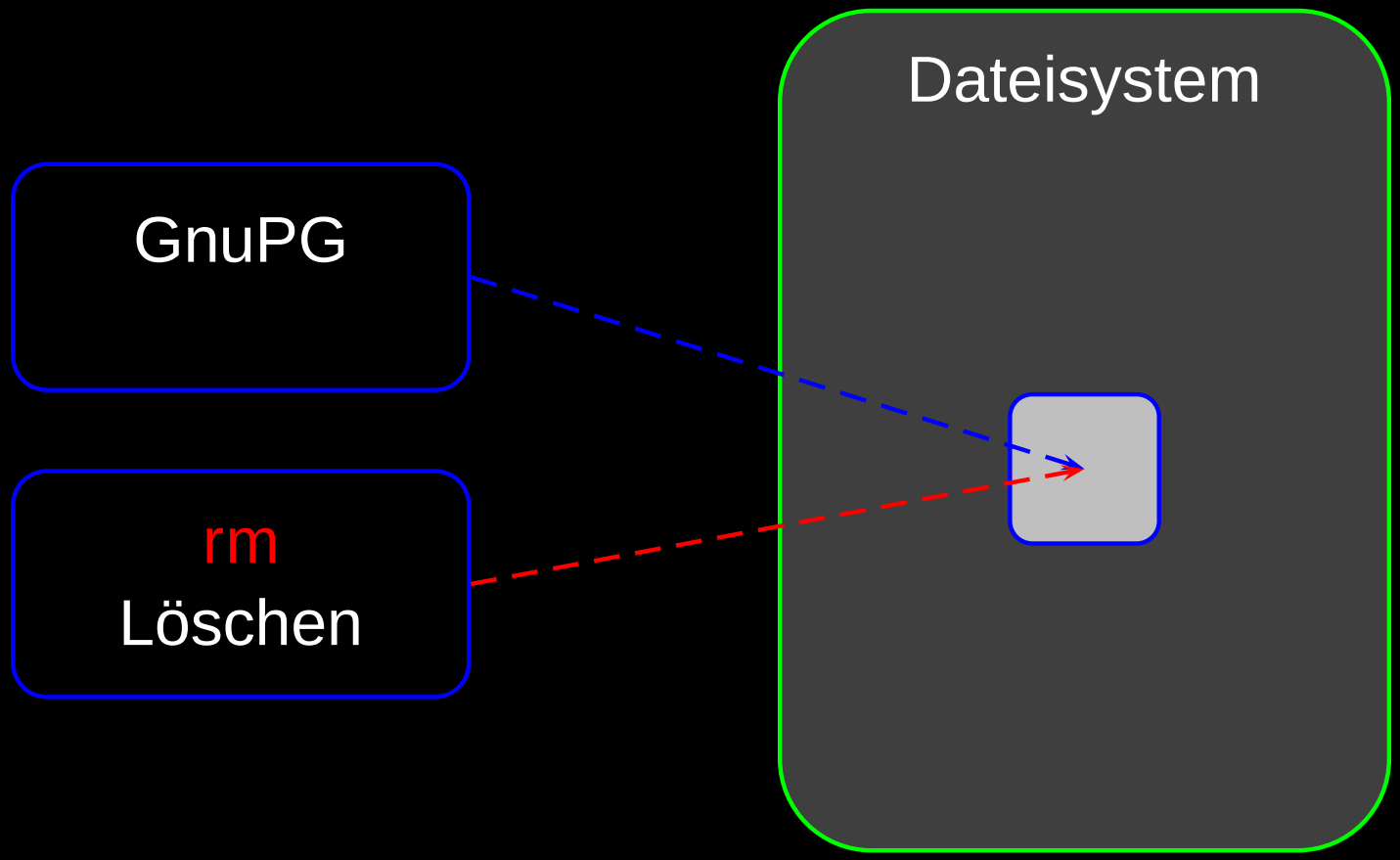
Was soll *nicht* besprochen werden?

- Netzsicherheit, insbesondere
- Firewalls und deren Konfiguration,
- Konzelationsverfahren jeglicher Art,
- Ausfallsicherheit.

Motivation



Motivation



Charakterisierung eines Angriffs

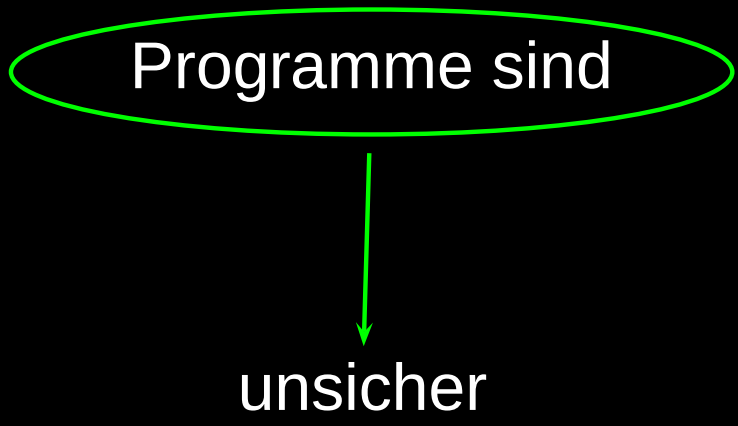
- Der Angreifer erringt Kontrolle über ein laufendes Programm.
- Der Programm-Code wird durch einen Angreifer unbemerkt modifiziert.
- Ein Programm läuft amog.

Charakterisierung eines Angriffs

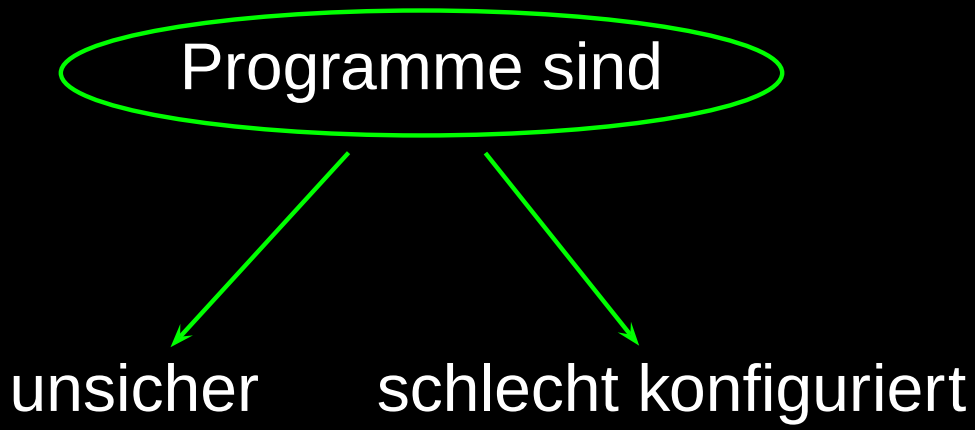
- Der Angreifer erringt Kontrolle über ein laufendes Programm.
- Der Programm-Code wird durch einen Angreifer unbemerkt modifiziert.
- Ein Programm läuft amog.

Schuld sind meistens Programme!

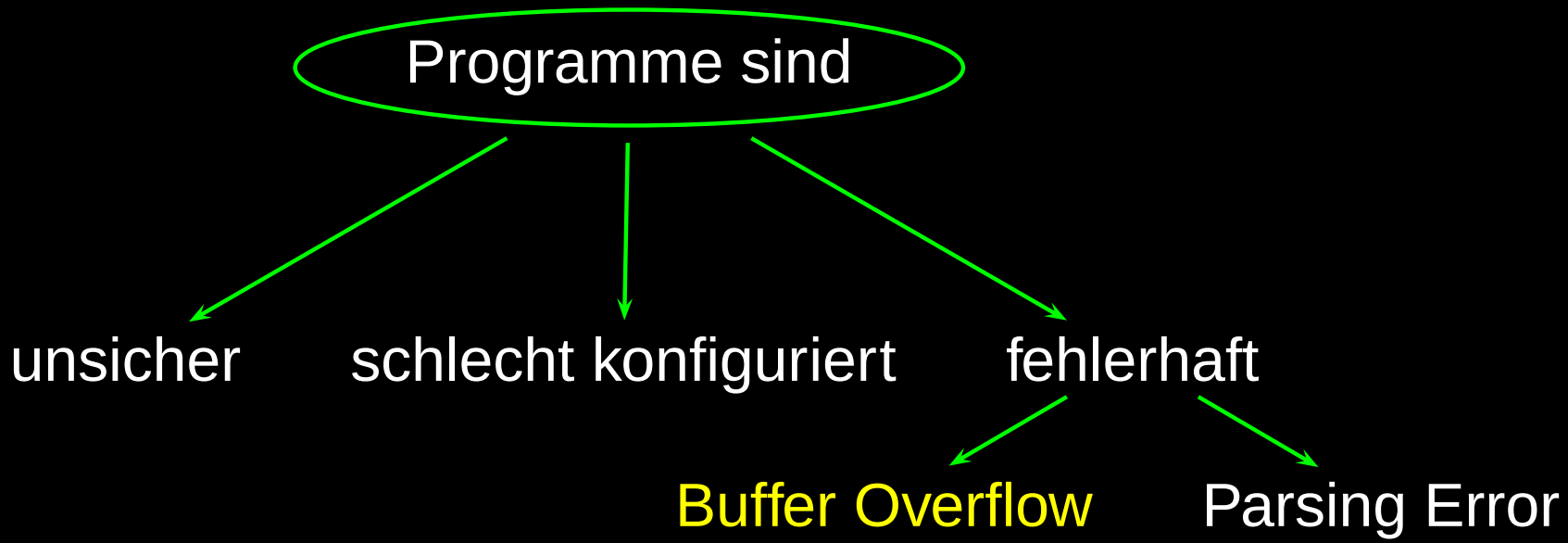
Bekannte Ursachen



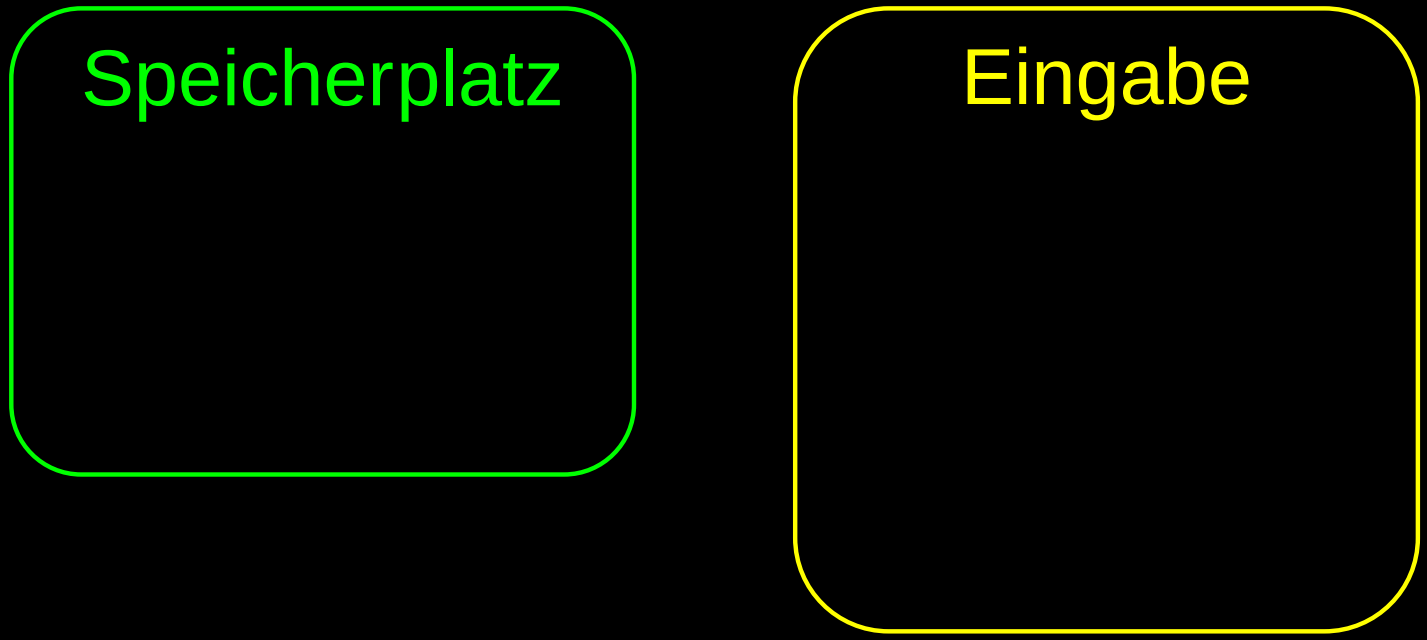
Bekannte Ursachen



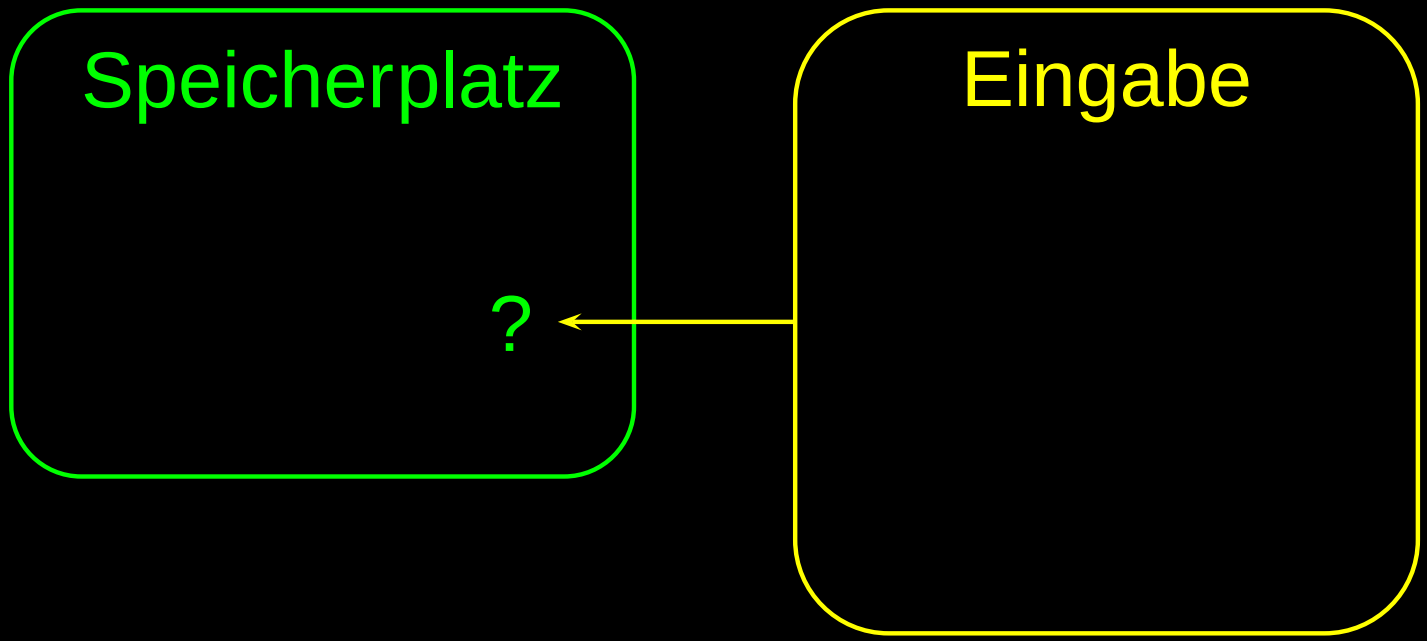
Bekannte Ursachen



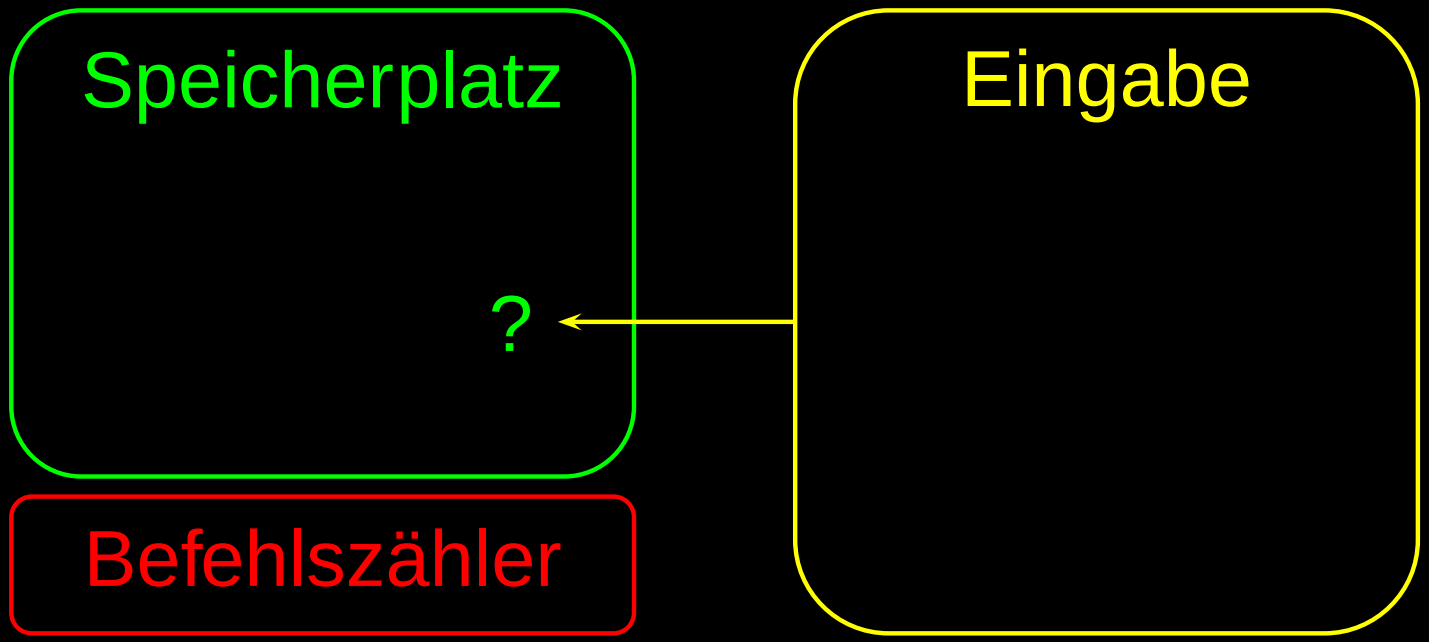
Buffer Overflow



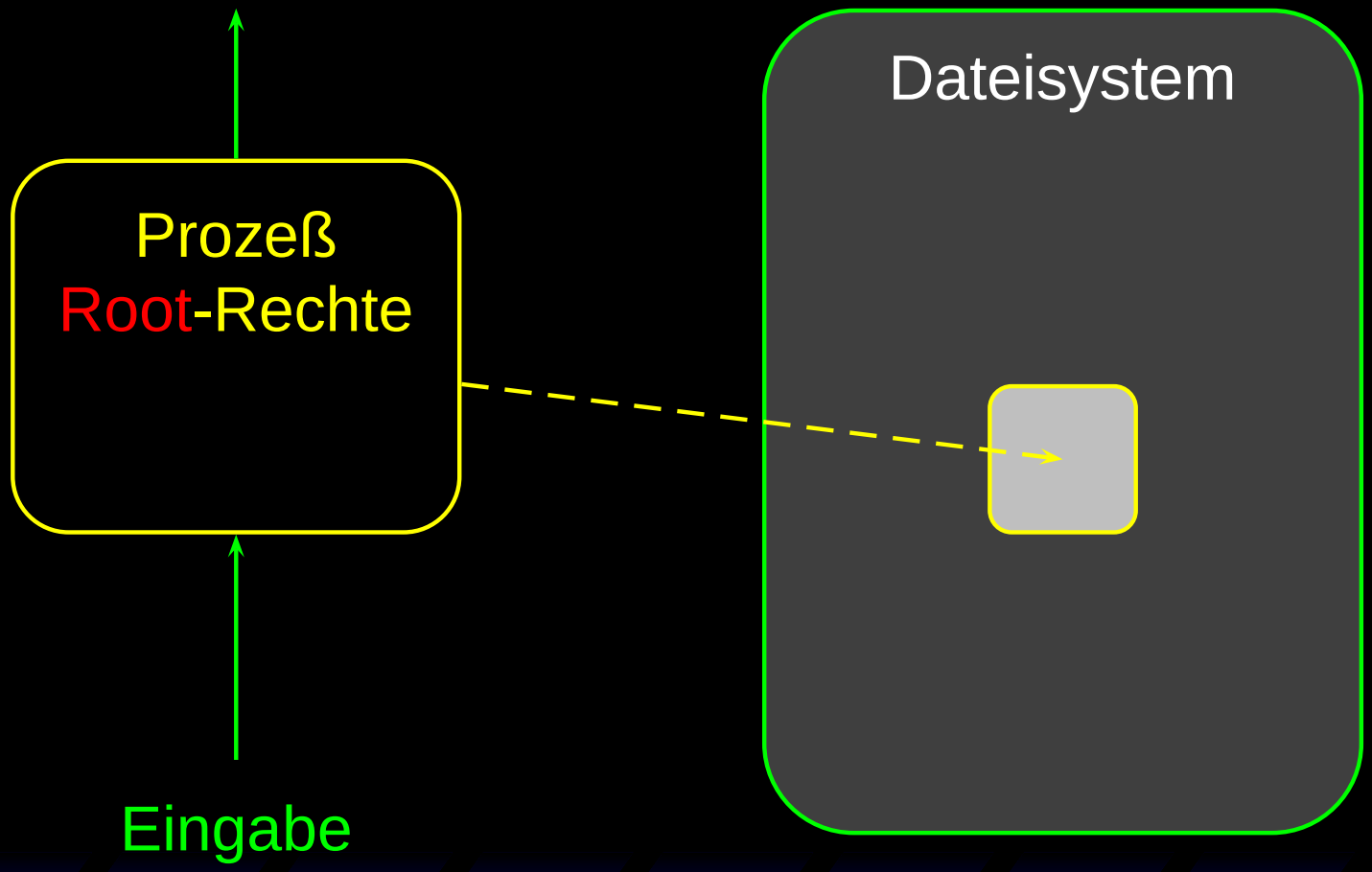
Buffer Overflow



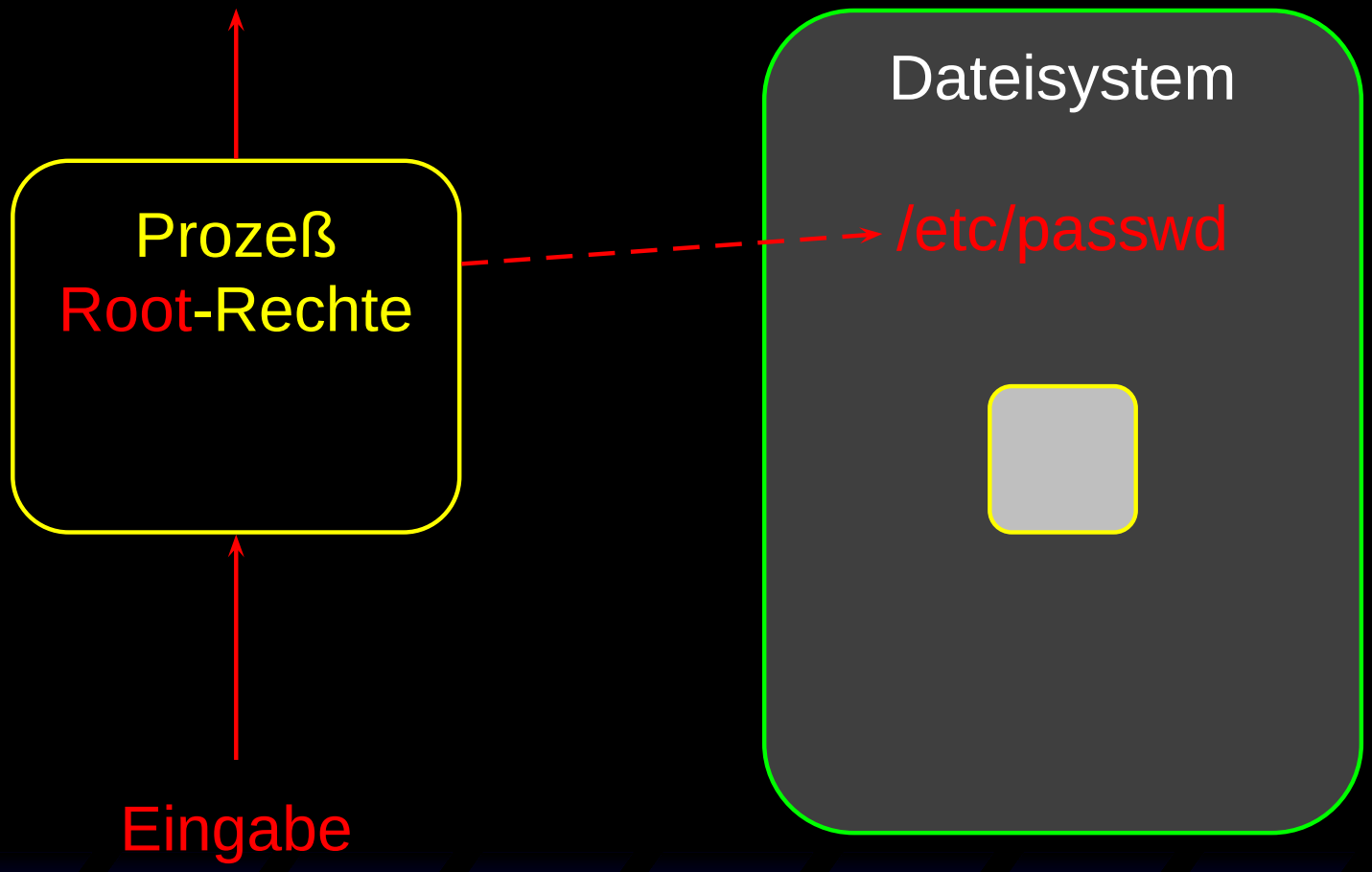
Buffer Overflow



Parsing Error



Parsing Error



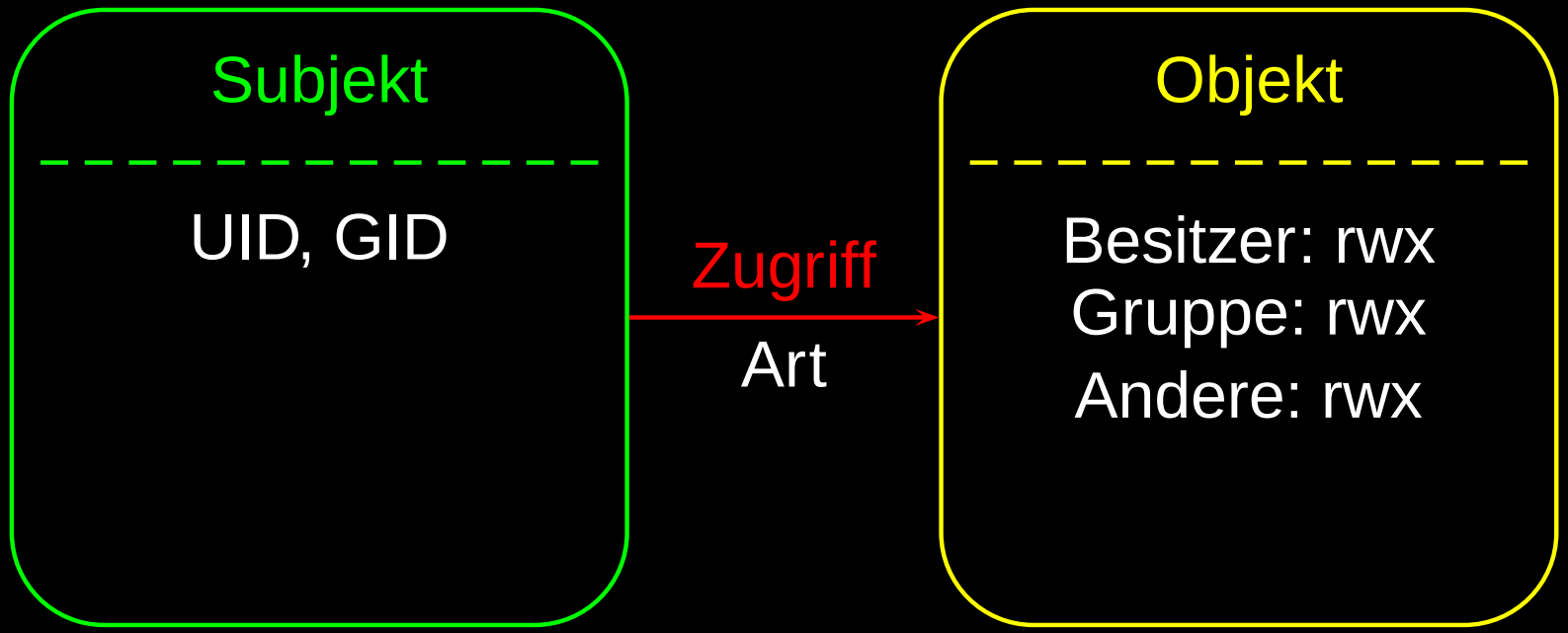
Was ist als kritisch zu betrachten?

Der Standard-Kern bietet. . .

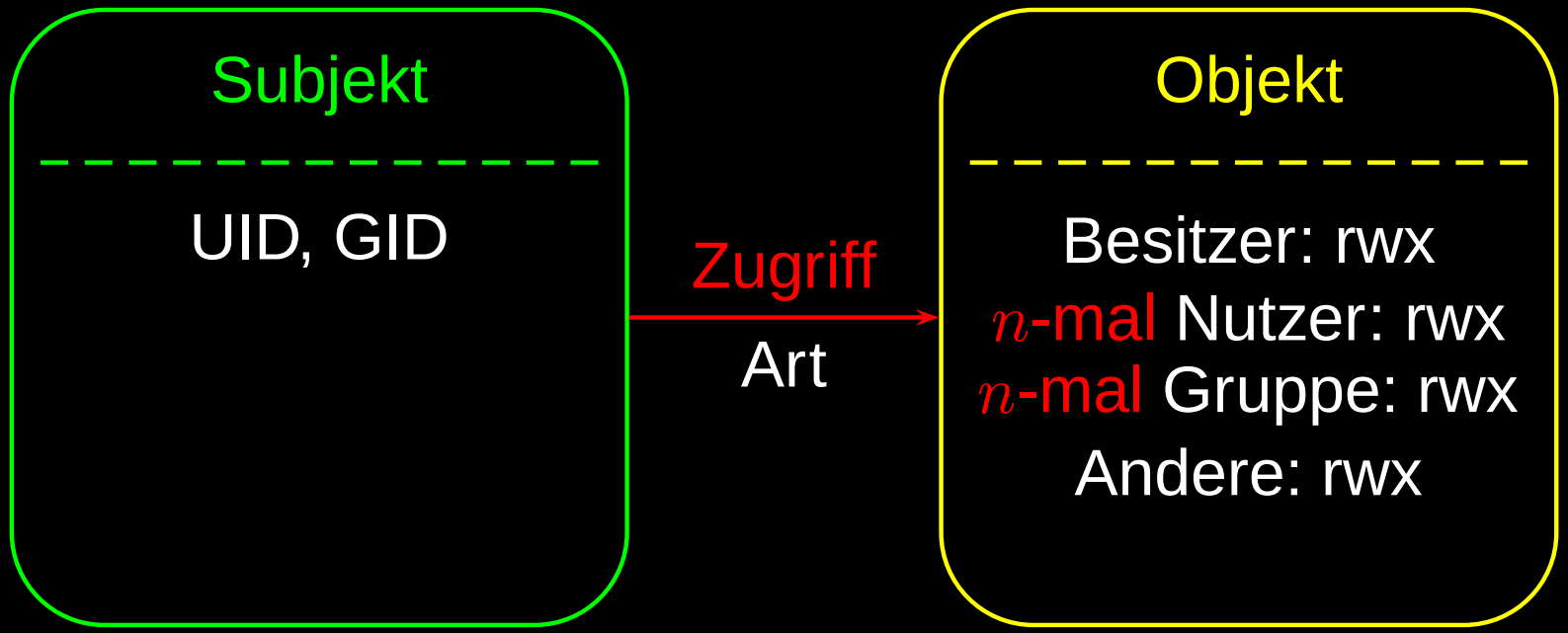
- zu geringe Ganularität,
- Discretionary Access Control (DAC),
- einen allmächtigen Administrator-Account mit festgelegter UID (root, 0).

Kontrollierter Zugang

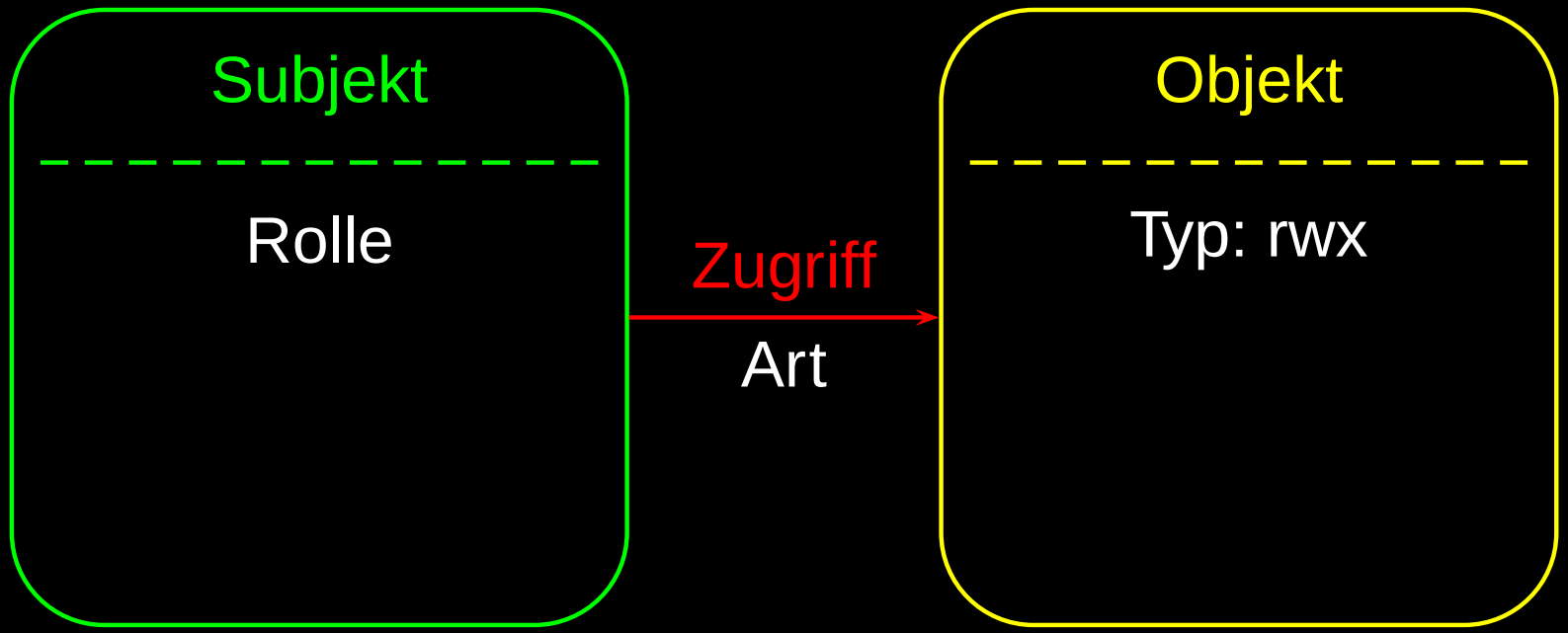
Standard-Kern



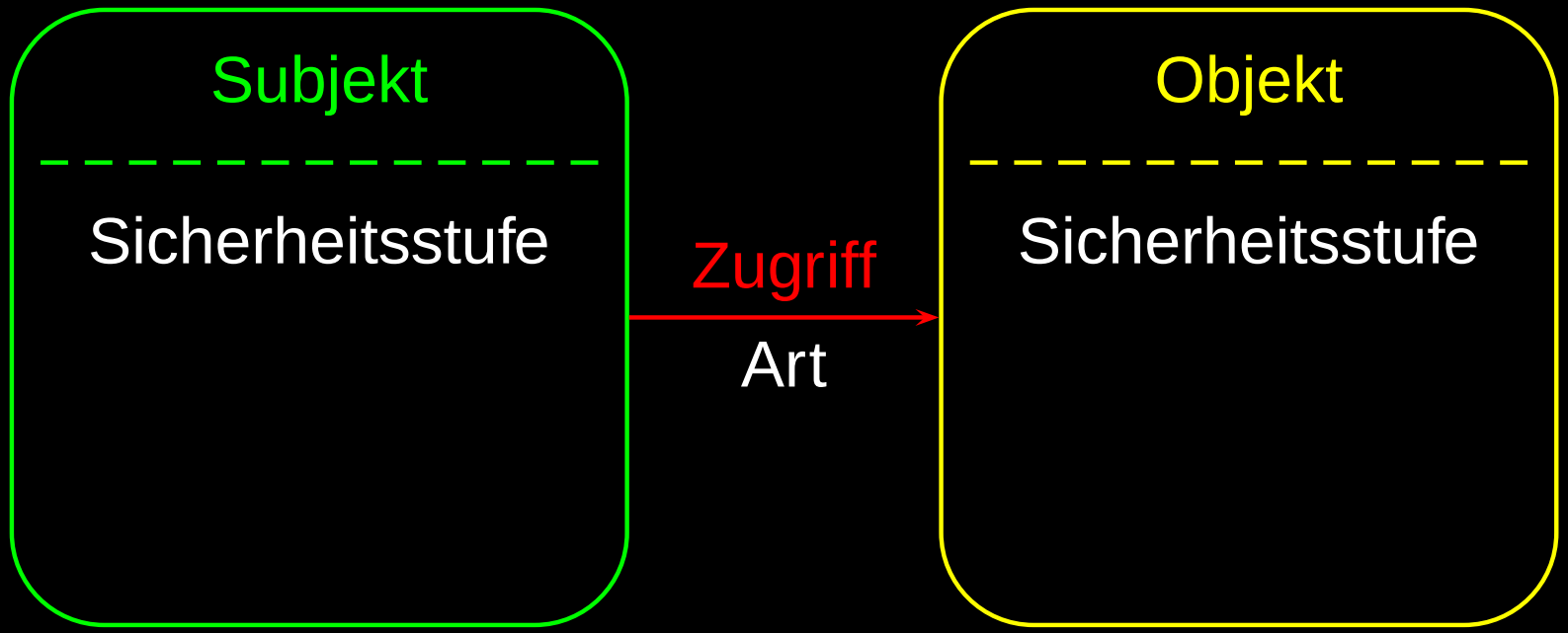
Access Control List



Role based Access Control



Bell-La Padula
Mandatory Access Control



Konkrete Implementationen

Linux Security Modules (LSM)

- Rahmenwerk für ein Modul
- Untermodule vom übergeordneten abhängig
- Performanz statt Sicherheit
- pot. Schnittstelle für neue Viren und Würmer
- integraler Bestandteil der 2.6er Kern-Reihe

Linux Intrusion Detection System (LIDS)

- unterstützt LSM
- „Access Control Lists“ für Dateisystem
- Prozesse als Handlungsträger (Subjekt)
- entmachtet den Administrator
- Aufgabendelegation nicht oder schwer möglich

GrSecurity

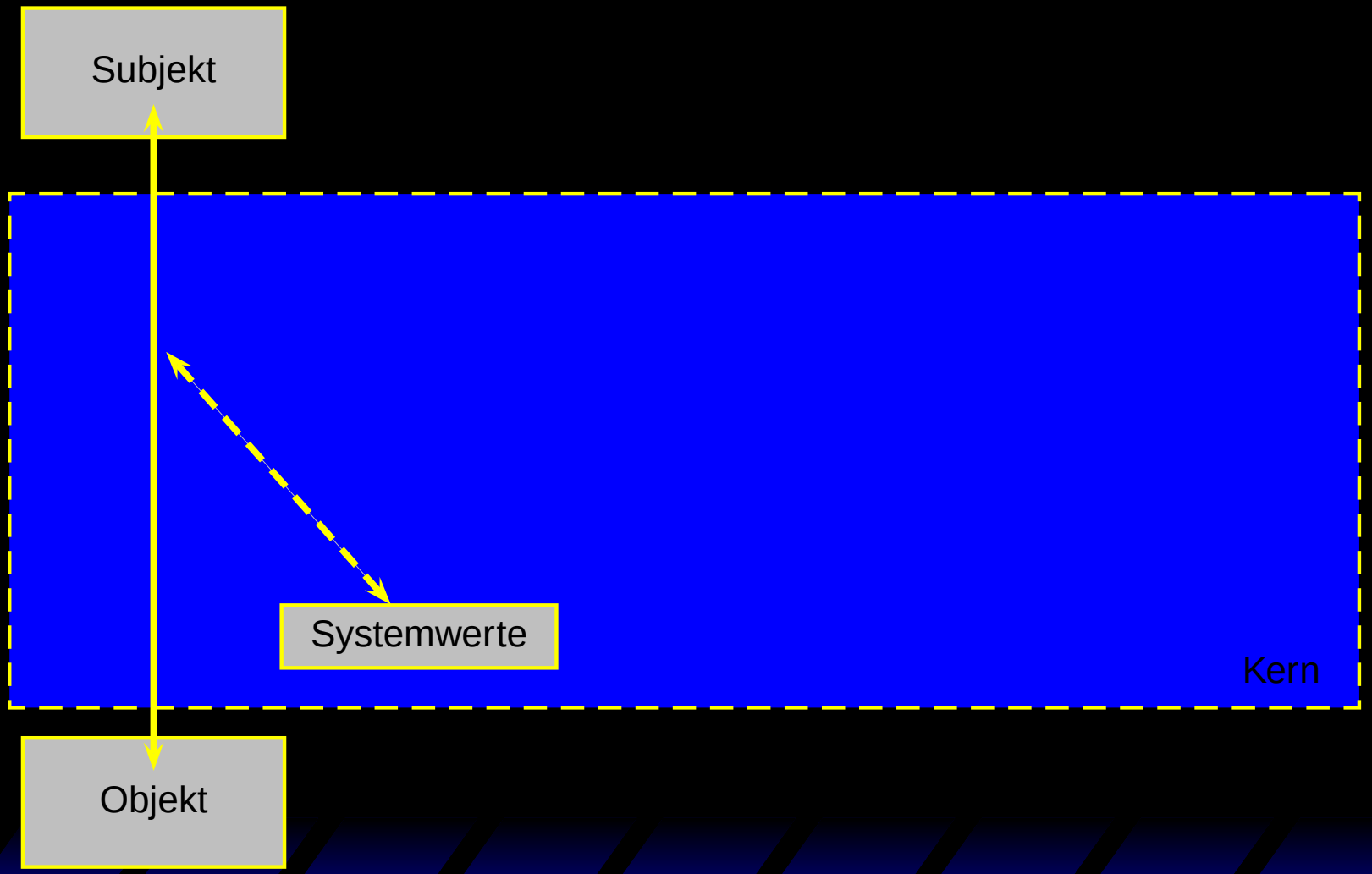
- Bündel aus Sicherheits-Patches (PaX, Openwall,. . .)
- Rollen-basierte Zugangskontrolle (RBAC)
- Aufgabendelegation mit Rollen möglich
- „Access Control Lists“ für Dateisystem
- entmachtet den Administrator
- keine Unterstützung von LSM

Rule Set Based Access Control

- Rahmenwerk wie LSM
- Sicherheitsmodelle: ACL, RC, AUTH, MAC
- Einführung neuer Subjekttypen: Sokets. . .
- Aufgabendelegation mit div. Sicherheitsmodellen möglich
- entmachtet den Administrator
- keine Unterstützung von LSM

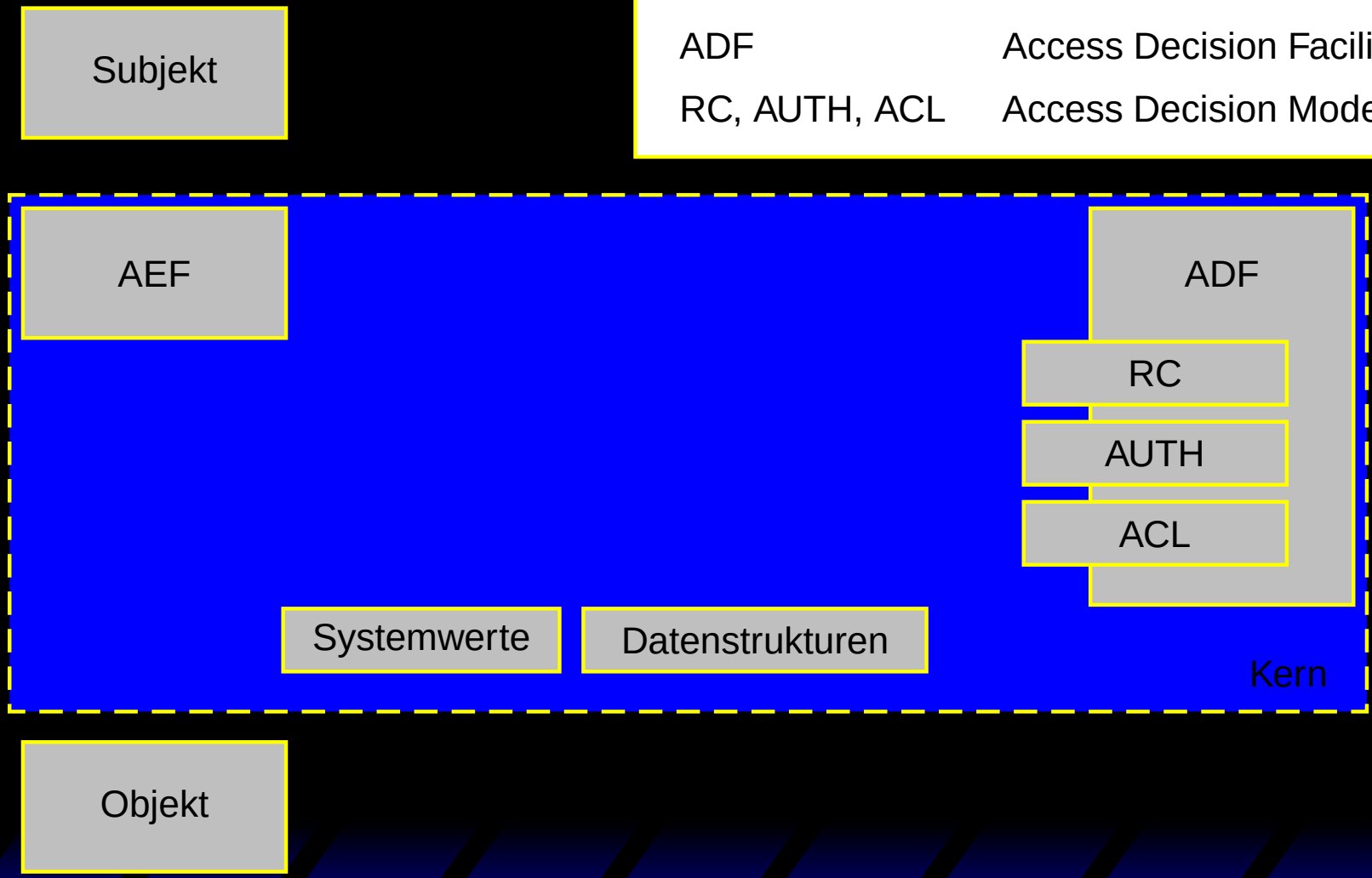
Annäherung an RSBAC

Verfahrensweise im Kern (AEF)



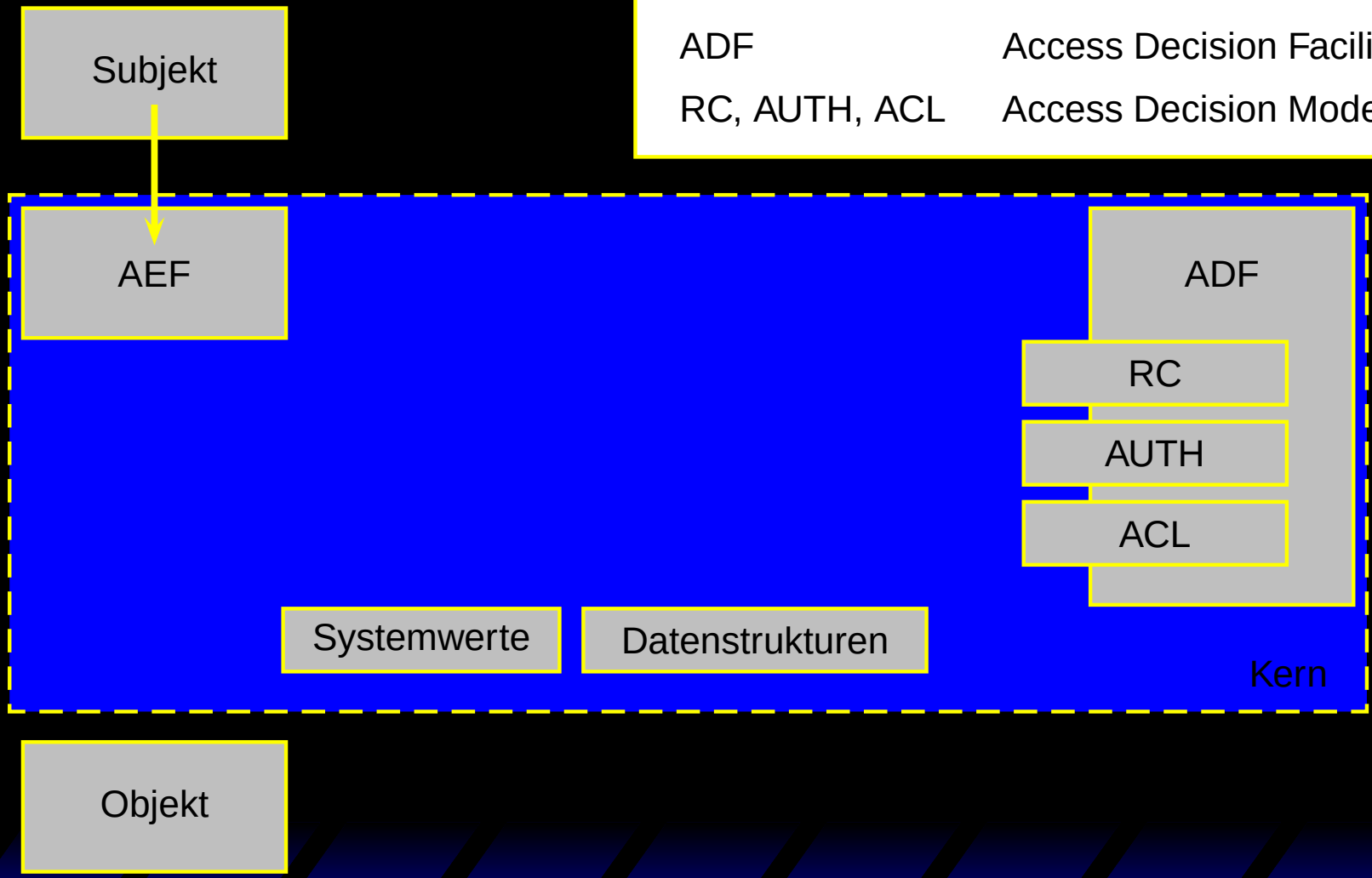
Verfahrensweise im Kern (AEF)

AEF	Access Enforcement Facility
ADF	Access Decision Facility
RC, AUTH, ACL	Access Decision Models



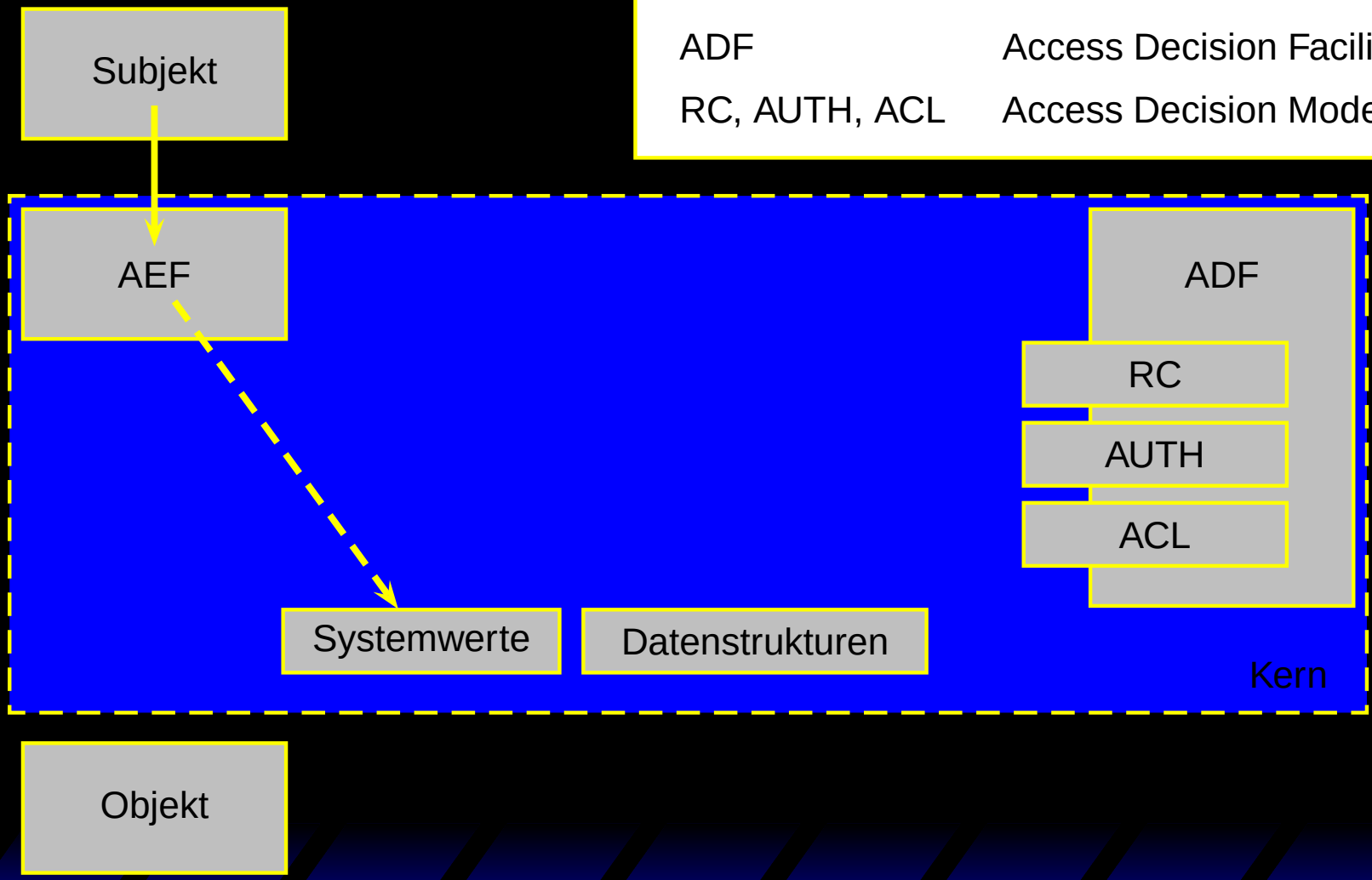
Verfahrensweise im Kern (AEF)

AEF	Access Enforcement Facility
ADF	Access Decision Facility
RC, AUTH, ACL	Access Decision Models



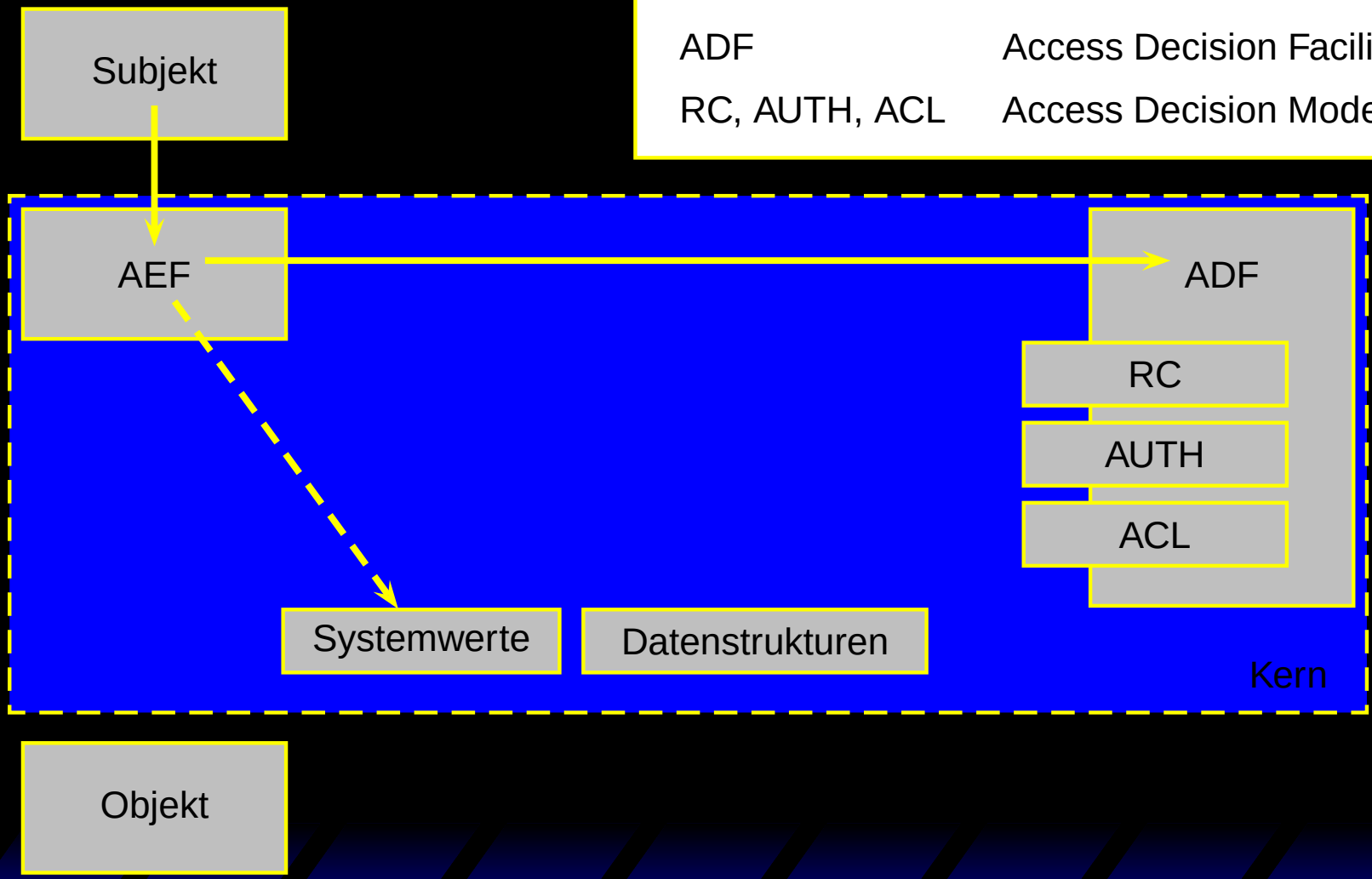
Verfahrensweise im Kern (AEF)

AEF	Access Enforcement Facility
ADF	Access Decision Facility
RC, AUTH, ACL	Access Decision Models



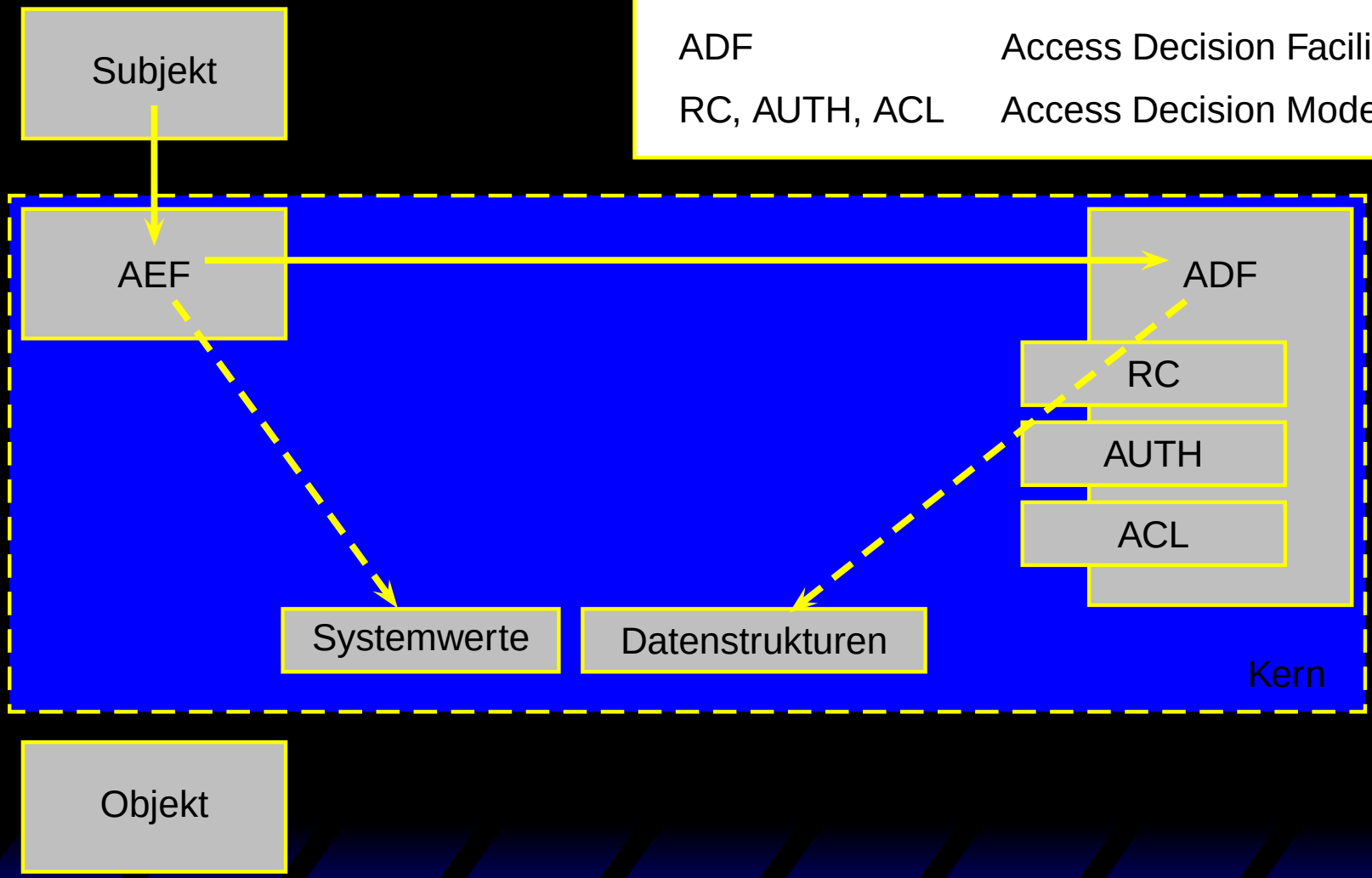
Verfahrensweise im Kern (AEF)

AEF	Access Enforcement Facility
ADF	Access Decision Facility
RC, AUTH, ACL	Access Decision Models



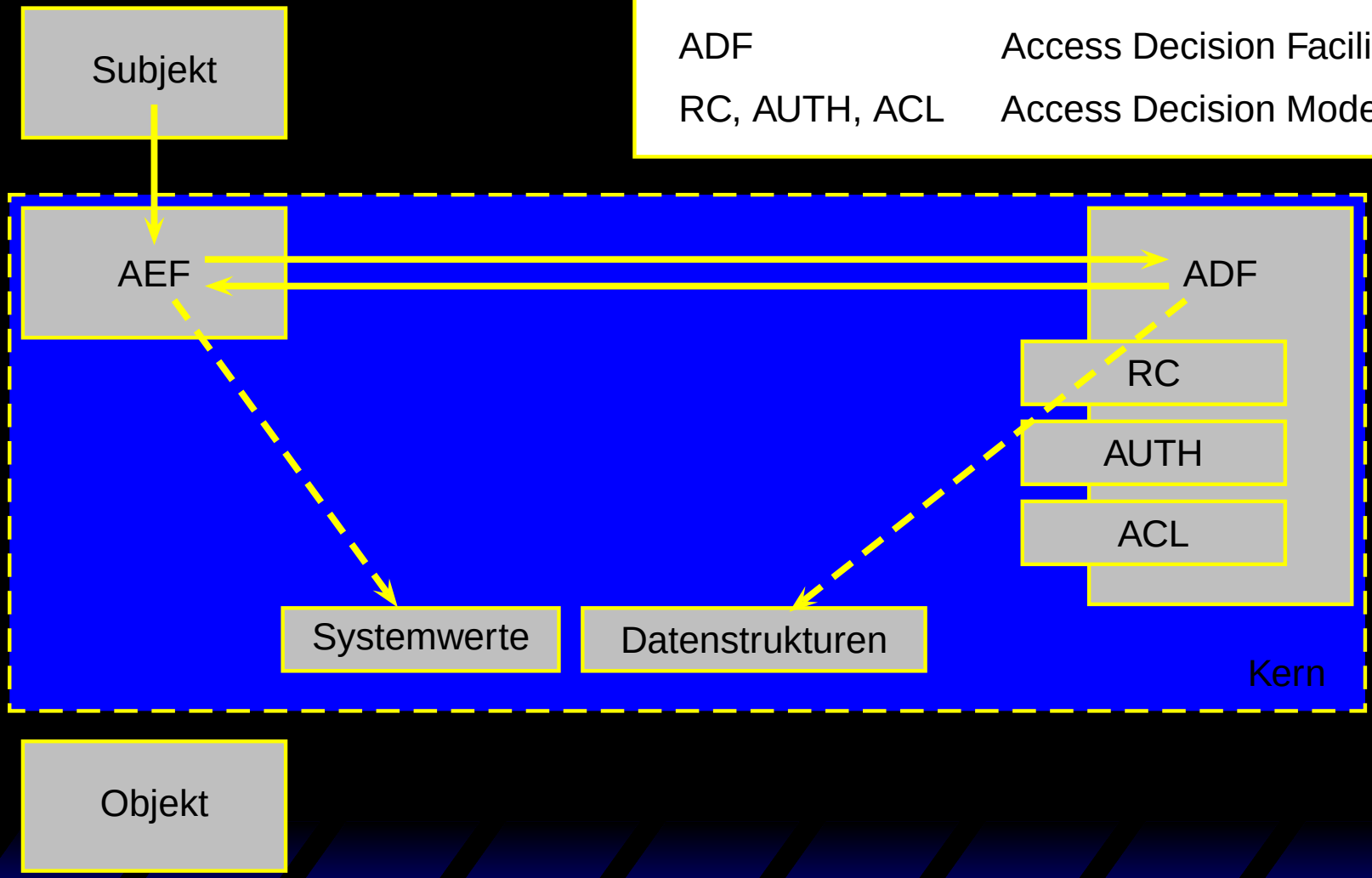
Verfahrensweise im Kern (AEF)

AEF	Access Enforcement Facility
ADF	Access Decision Facility
RC, AUTH, ACL	Access Decision Models



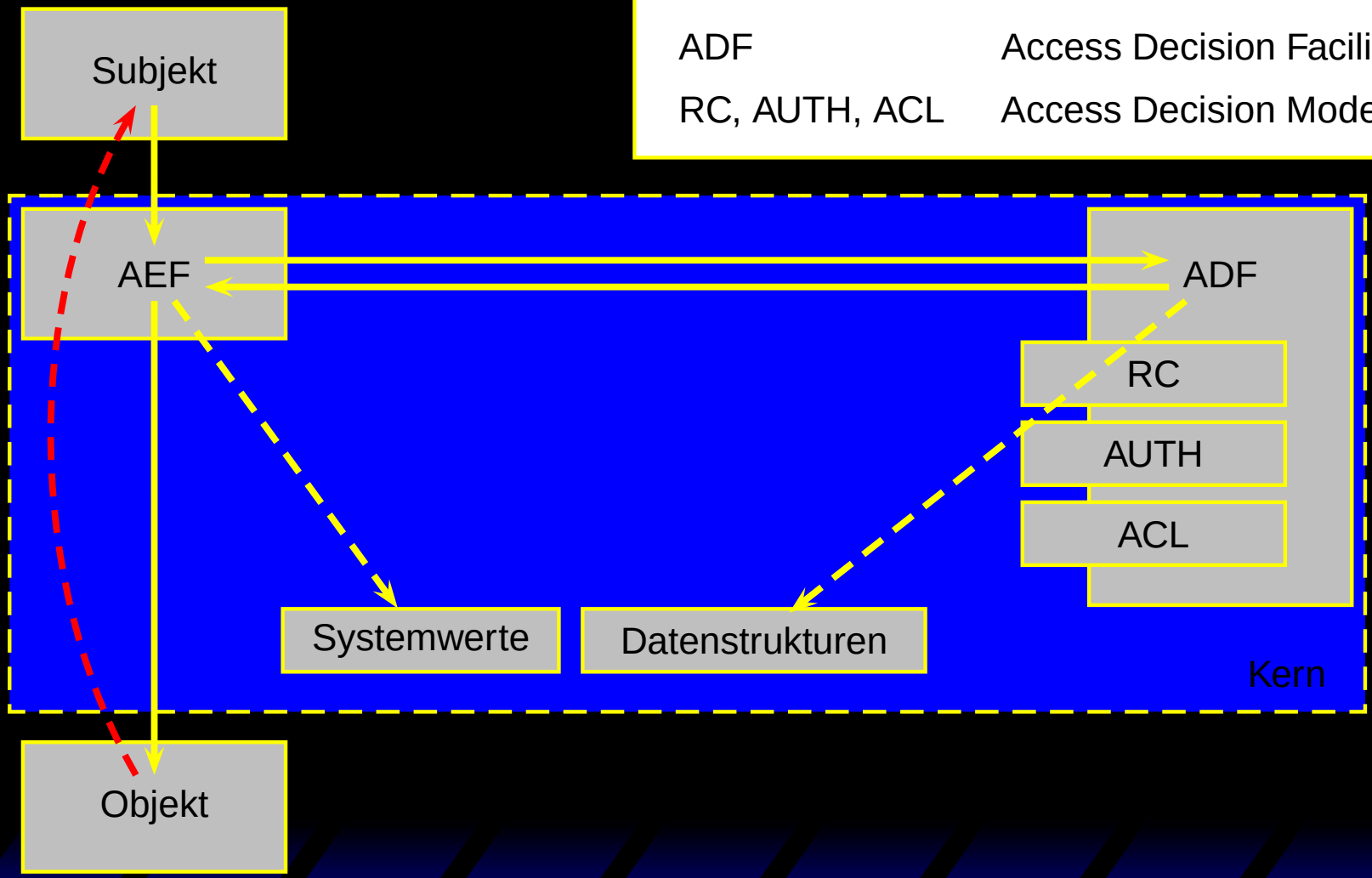
Verfahrensweise im Kern (AEF)

AEF	Access Enforcement Facility
ADF	Access Decision Facility
RC, AUTH, ACL	Access Decision Models

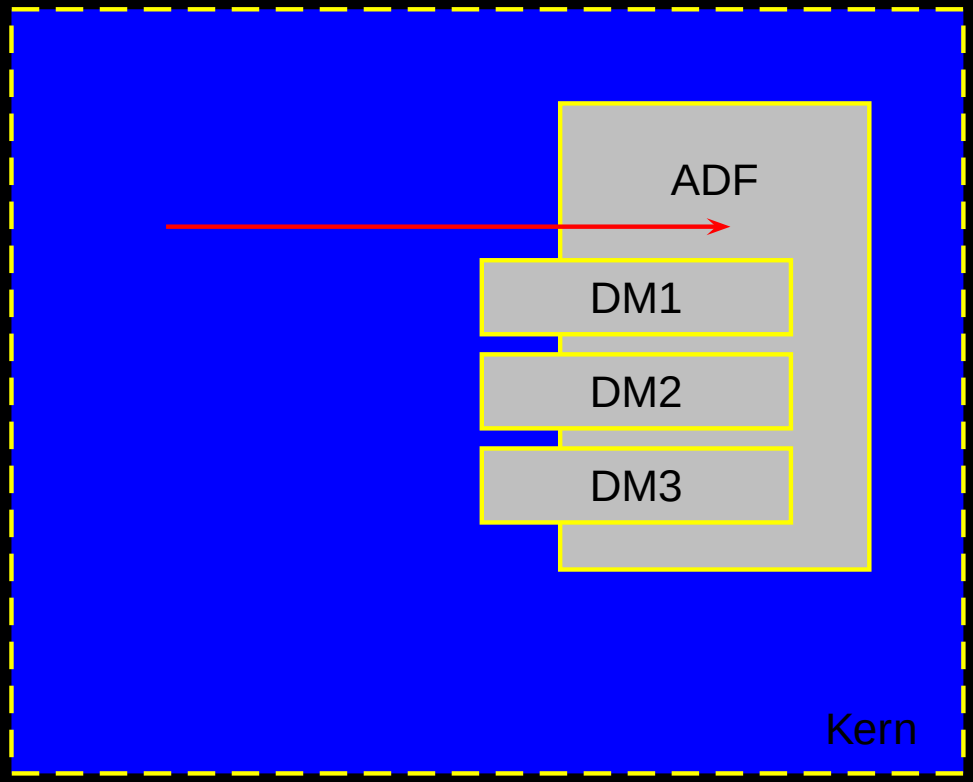


Verfahrensweise im Kern (AEF)

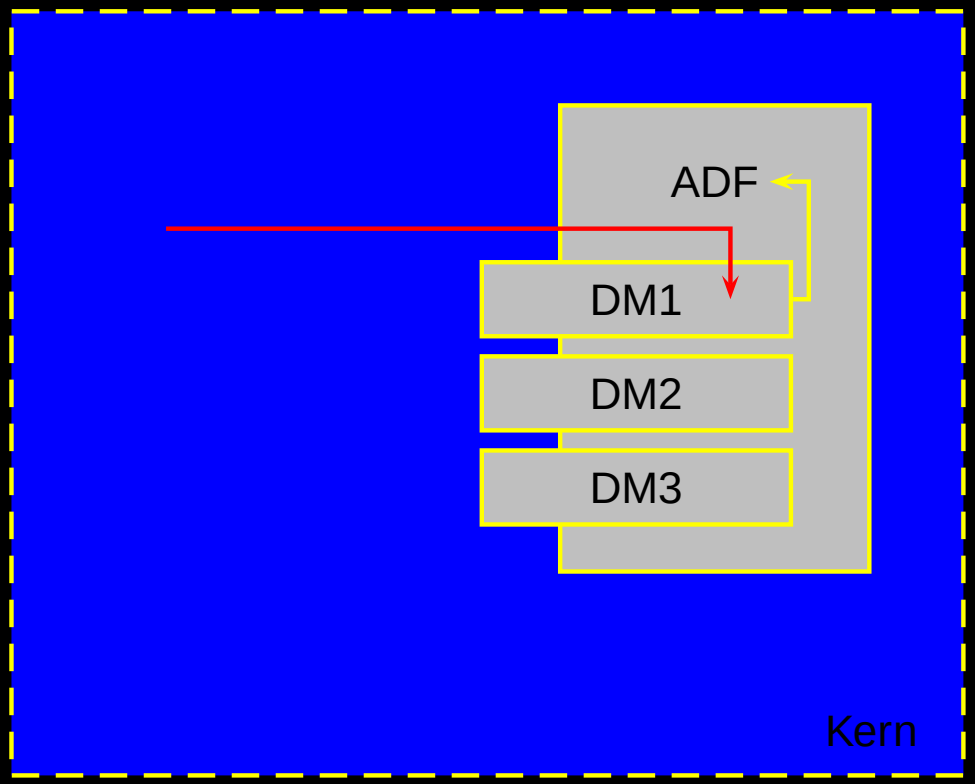
AEF	Access Enforcement Facility
ADF	Access Decision Facility
RC, AUTH, ACL	Access Decision Models



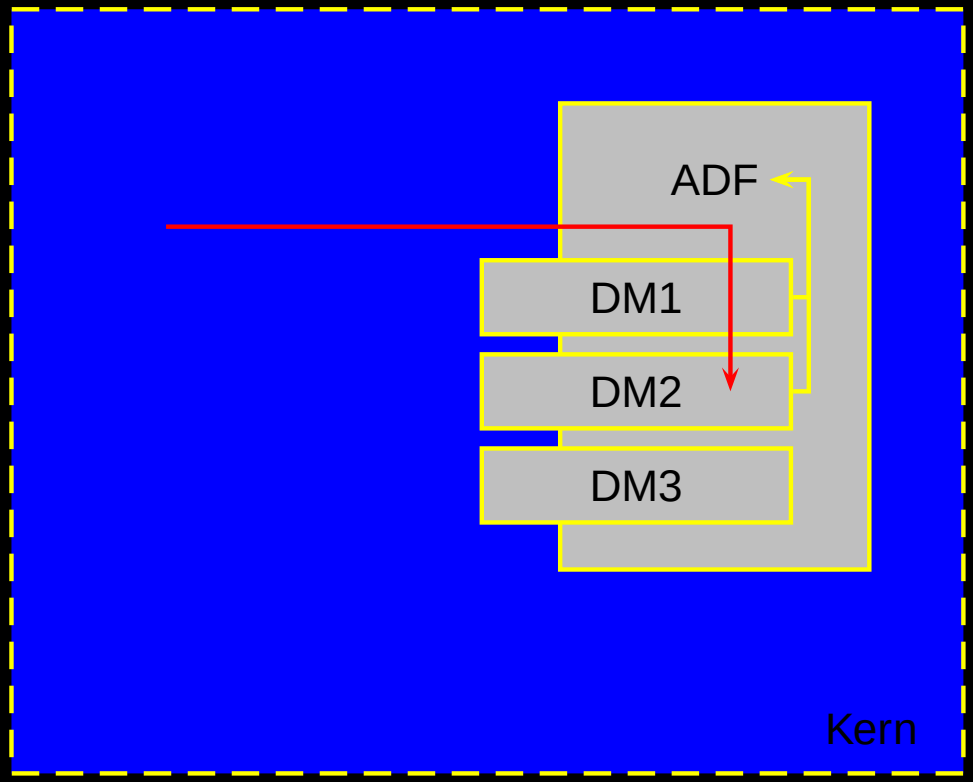
Entscheidungsfindung (ADF)



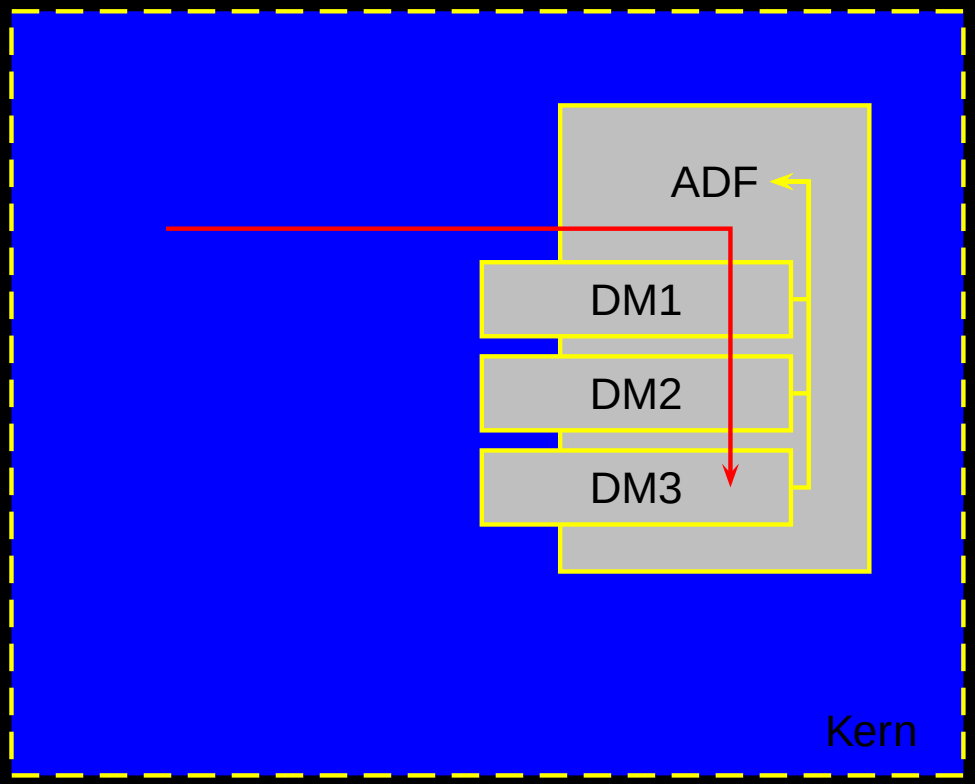
Entscheidungsfindung (ADF)



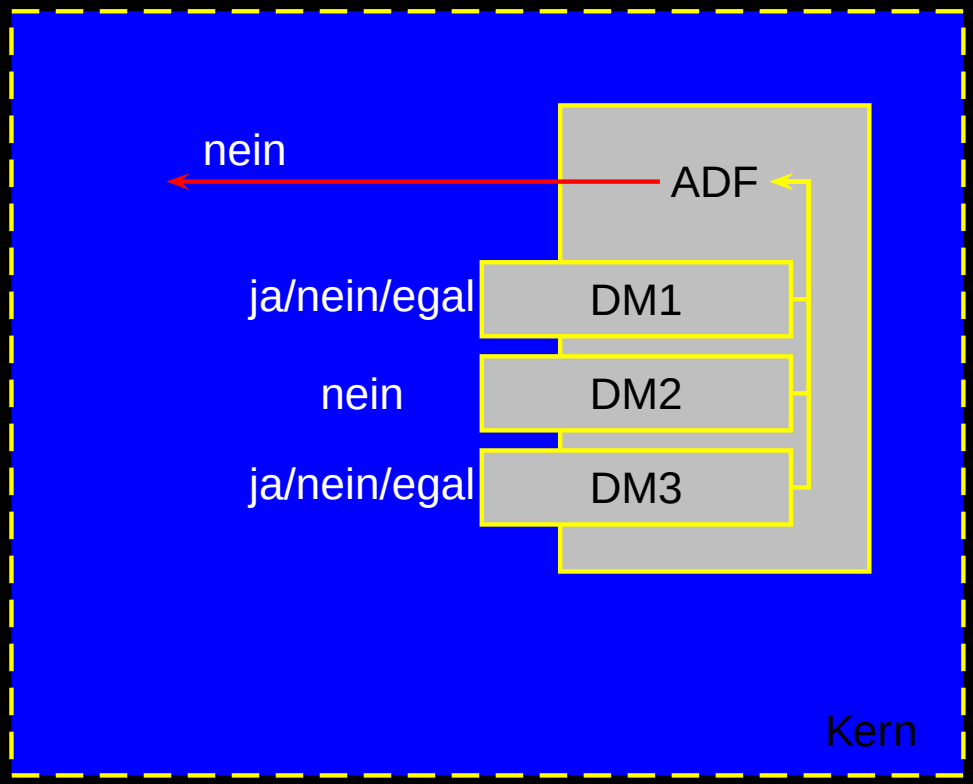
Entscheidungsfindung (ADF)



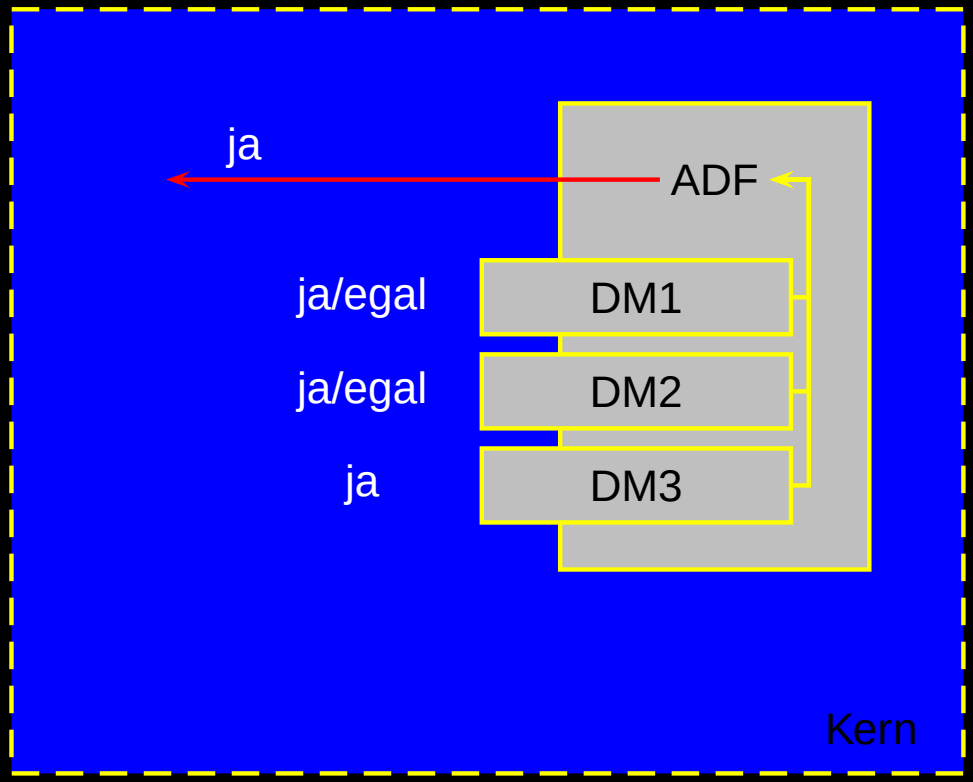
Entscheidungsfindung (ADF)



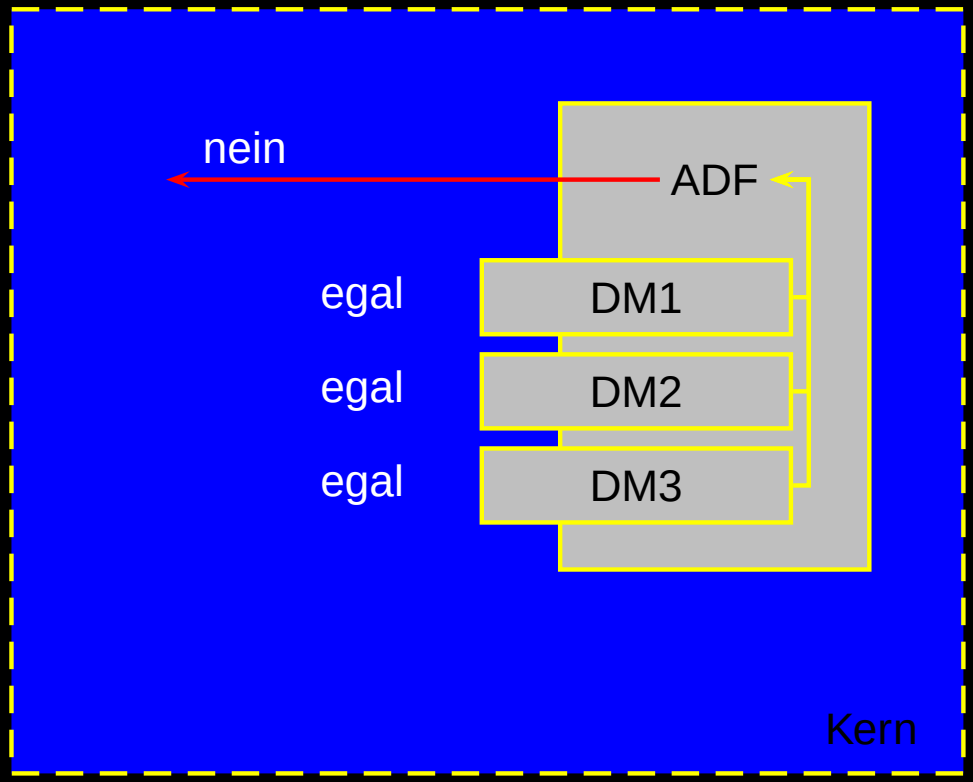
Entscheidungsfindung (ADF)



Entscheidungsfindung (ADF)



Entscheidungsfindung (ADF)



Zusammenfassend

- Vortrag sollte nur Geschmack anregen. . .
- Sicherheitsprobleme fangen am Endsystem an, nicht erst im Netz!
- Es gibt fertige Lösungen. . .
  - RSBAC: `http://www.rsbac.org/`
  - Adamantix: `http://www.adamantix.org/`
- Fragen: `http://lug-dd.schlittermann.de/`