FACULTEIT INGENIEURSWETENSCHAPPEN
EN ARCHITECTUUR

BOOSTING MVX SYSTEMS THROUGH MODERN OS EXTENSIONS

Lennert Franssens, student Industriële Wetenschappen in de Informatica

UNIVERSITEIT
GENT

OVERZICHT

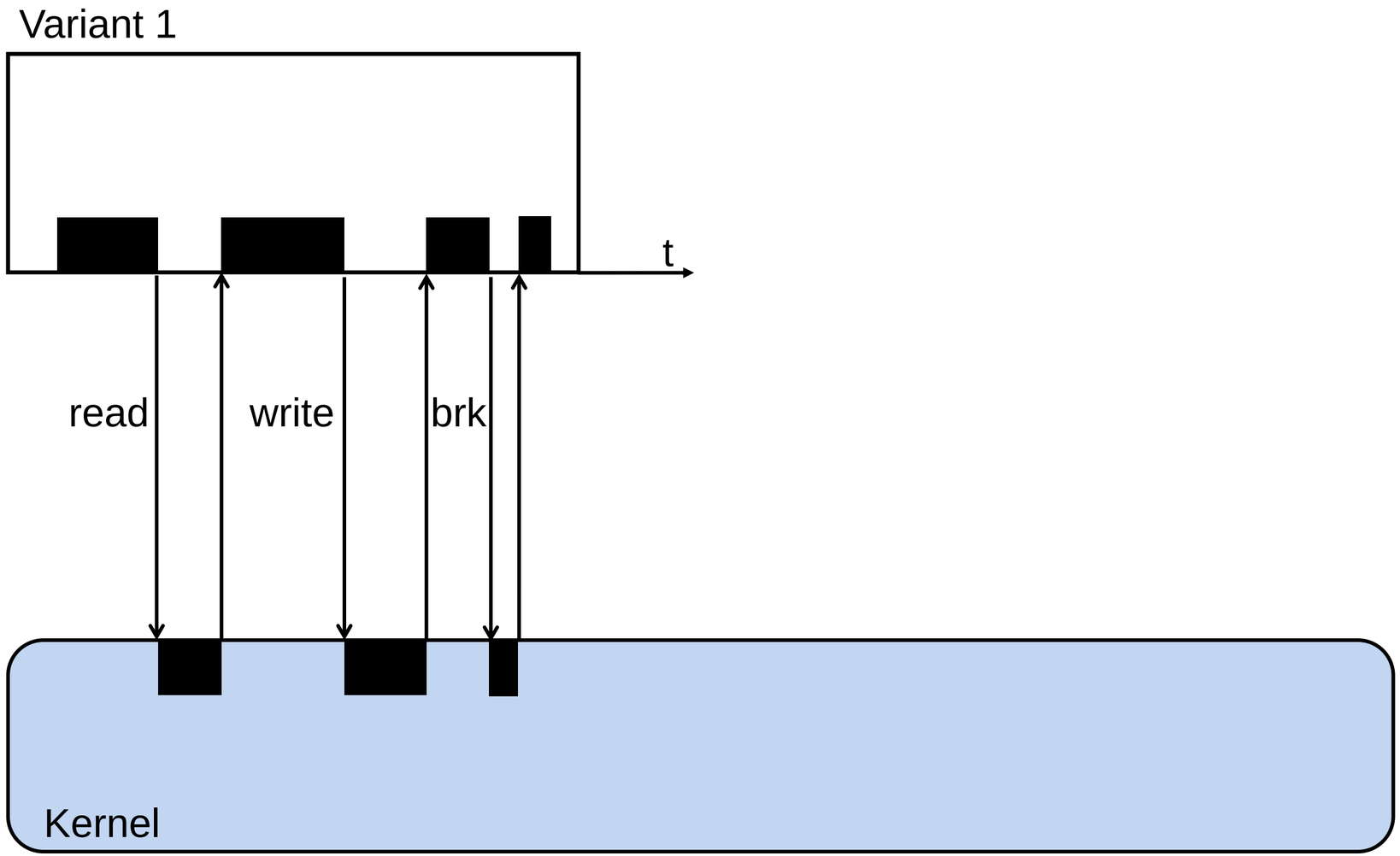
- MVEE
- ReMon met IP-MON
- Seccomp-BPF
- Nieuw design ReMon
- Veiligheid
- Tekortkomingen
- Testresultaten
- Conclusie
- Vragen

UNIVERSITEIT GENT

MVEE

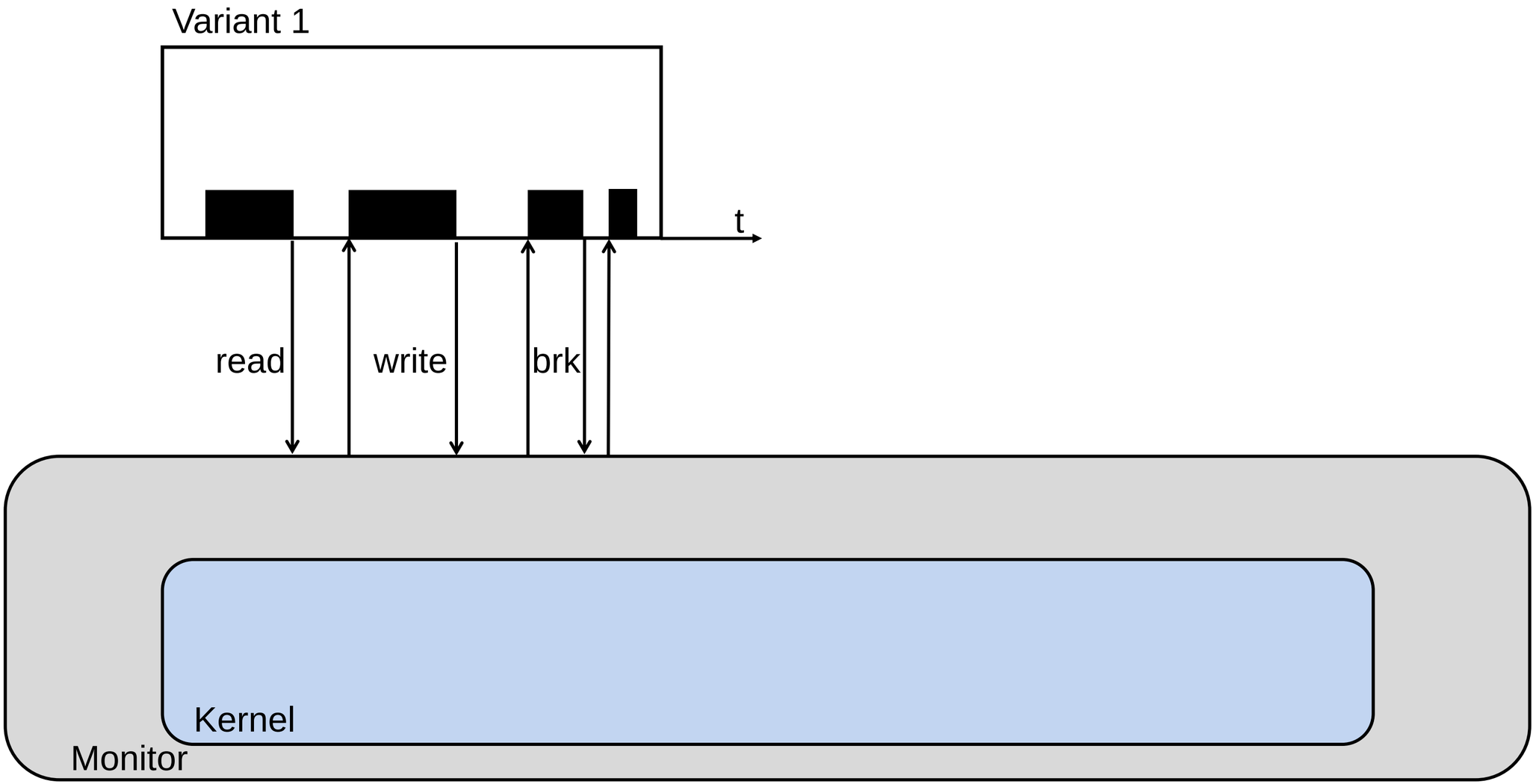
UNIVERSITEIT
GENT

MVEE



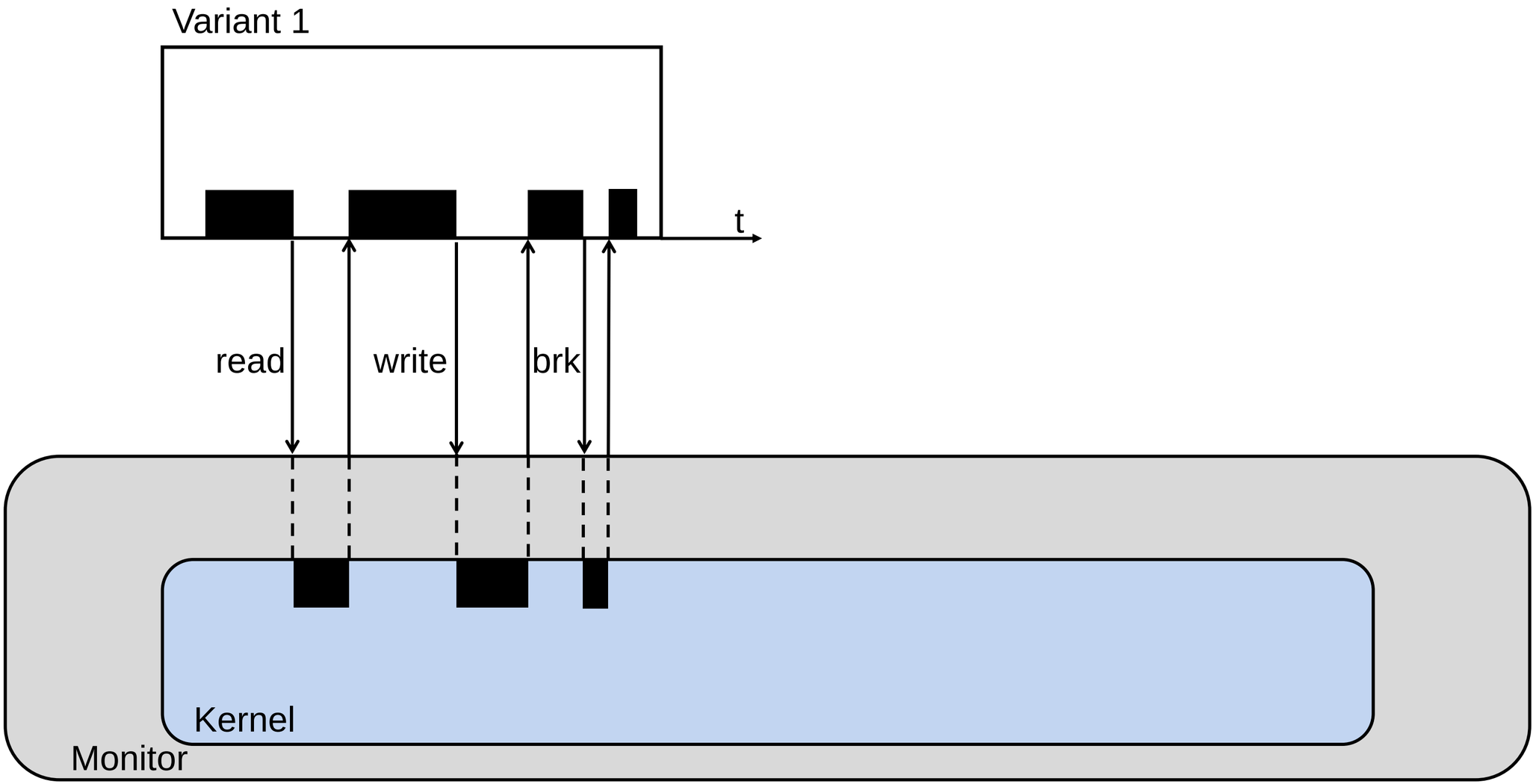
UNIVERSITEIT GENT

MONITOR – TRACER PROCES



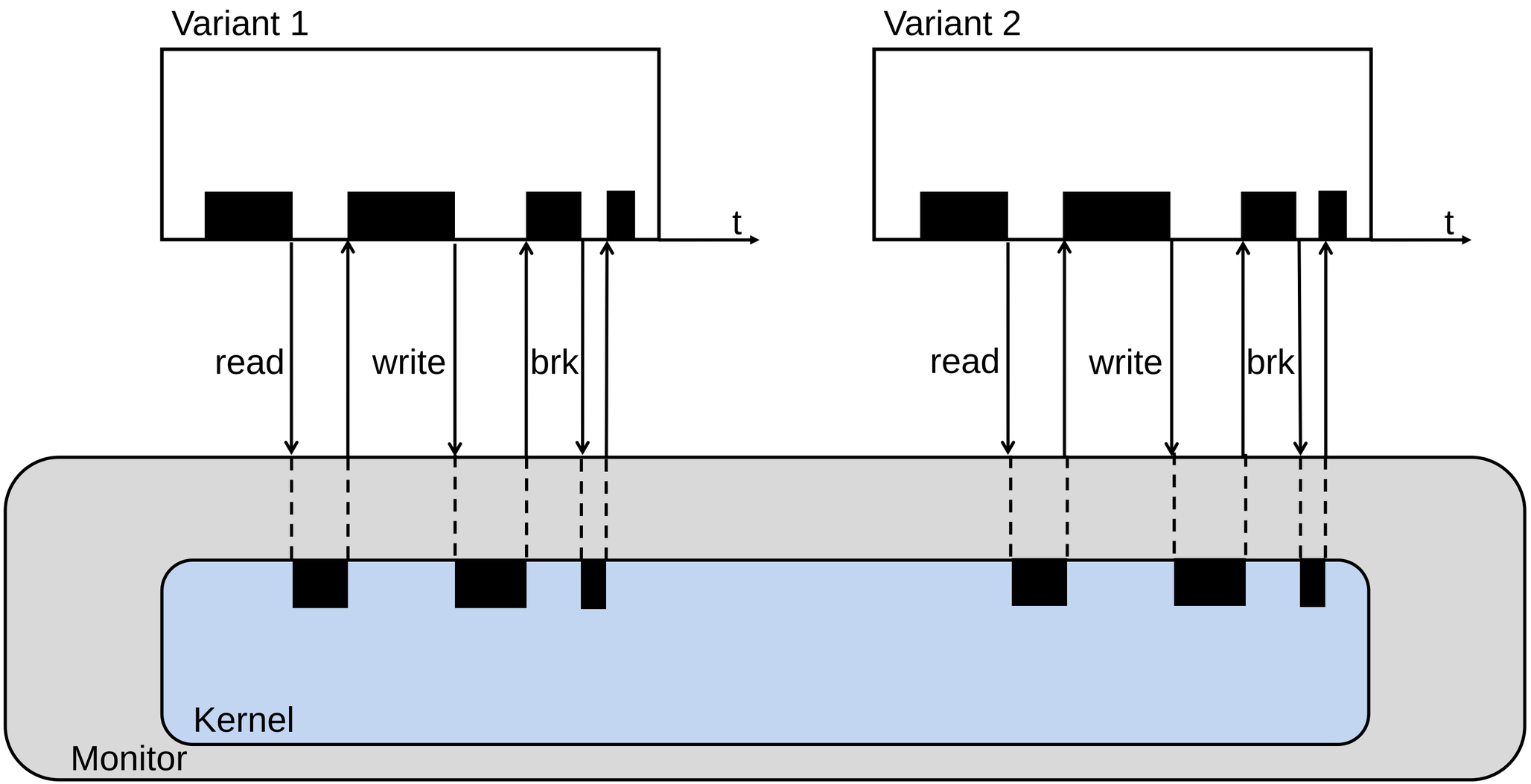
UNIVERSITEIT GENT

MONITOR – TRACER PROCES



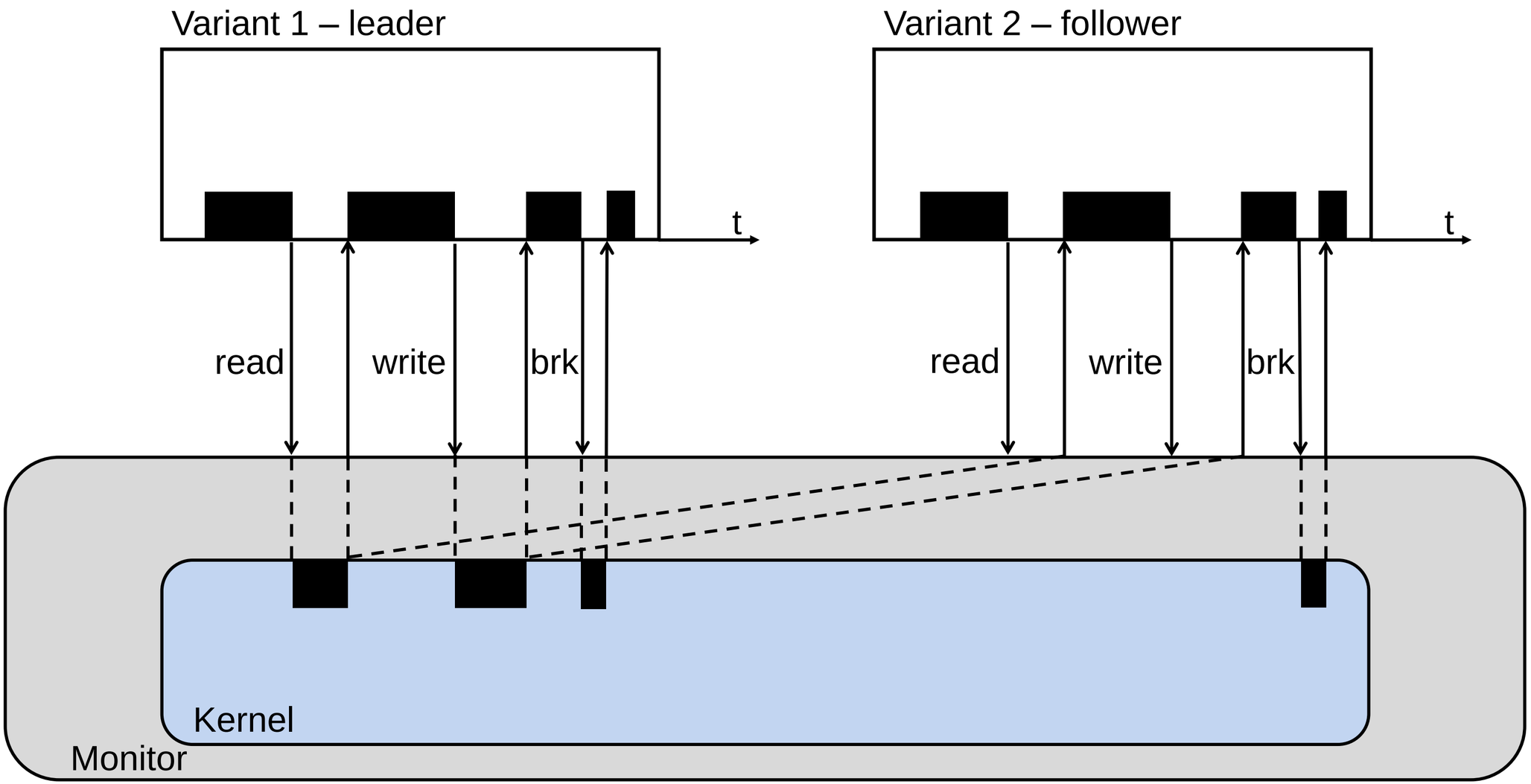
UNIVERSITEIT GENT

MONITOR – TRACER PROCES



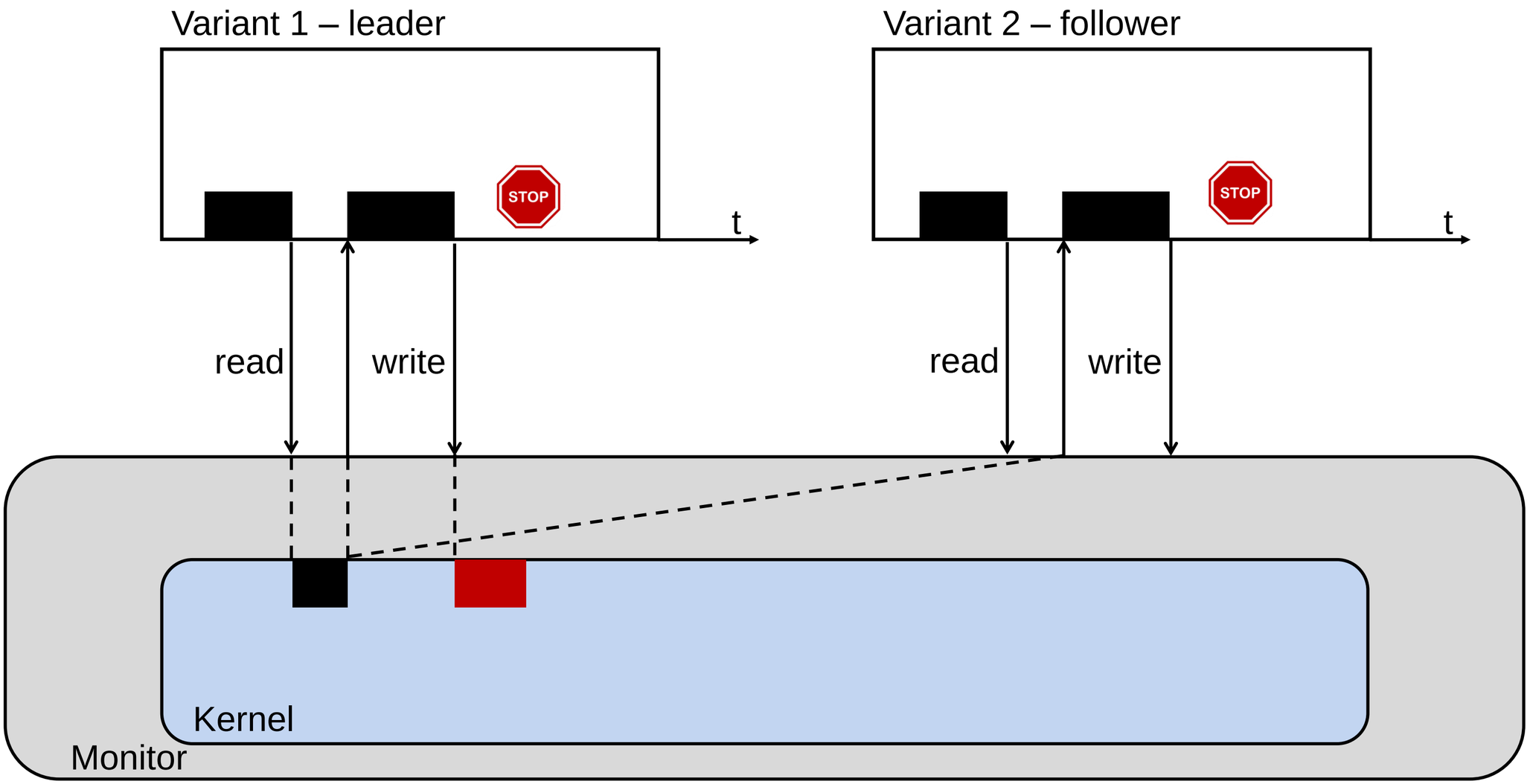
UNIVERSITEIT GENT

LEADER/FOLLOWER-MODEL VOOR IO REPLICATIE



UNIVERSITEIT GENT

DETECTIE VAN VERSCHIL IN GEDRAG



UNIVERSITEIT GENT

GROTE RUNTIME OVERHEAD

- Veel contextswitches
- Beveiliging boven snelheid

UNIVERSITEIT GENT

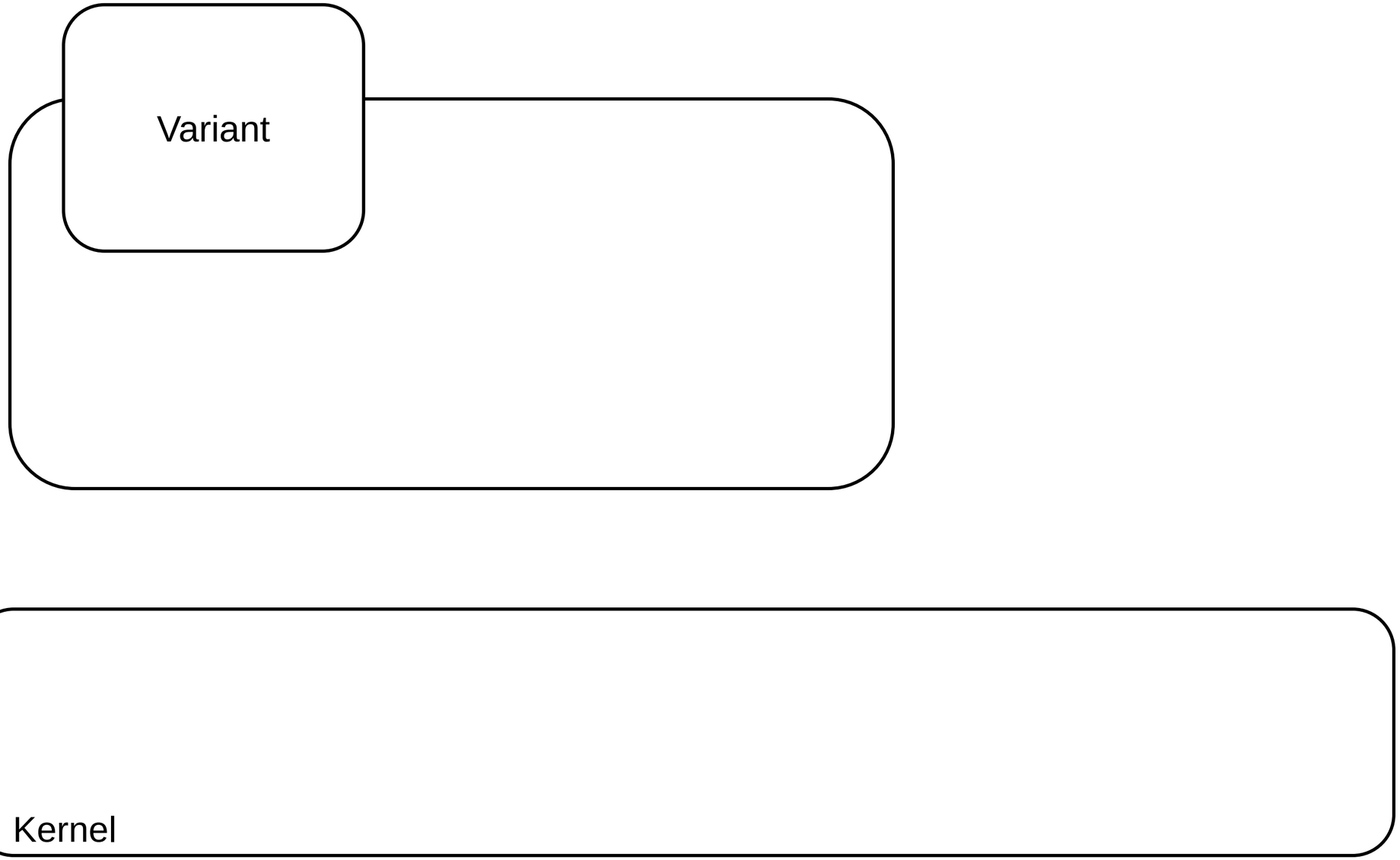
REMON

UNIVERSITEIT
GENT

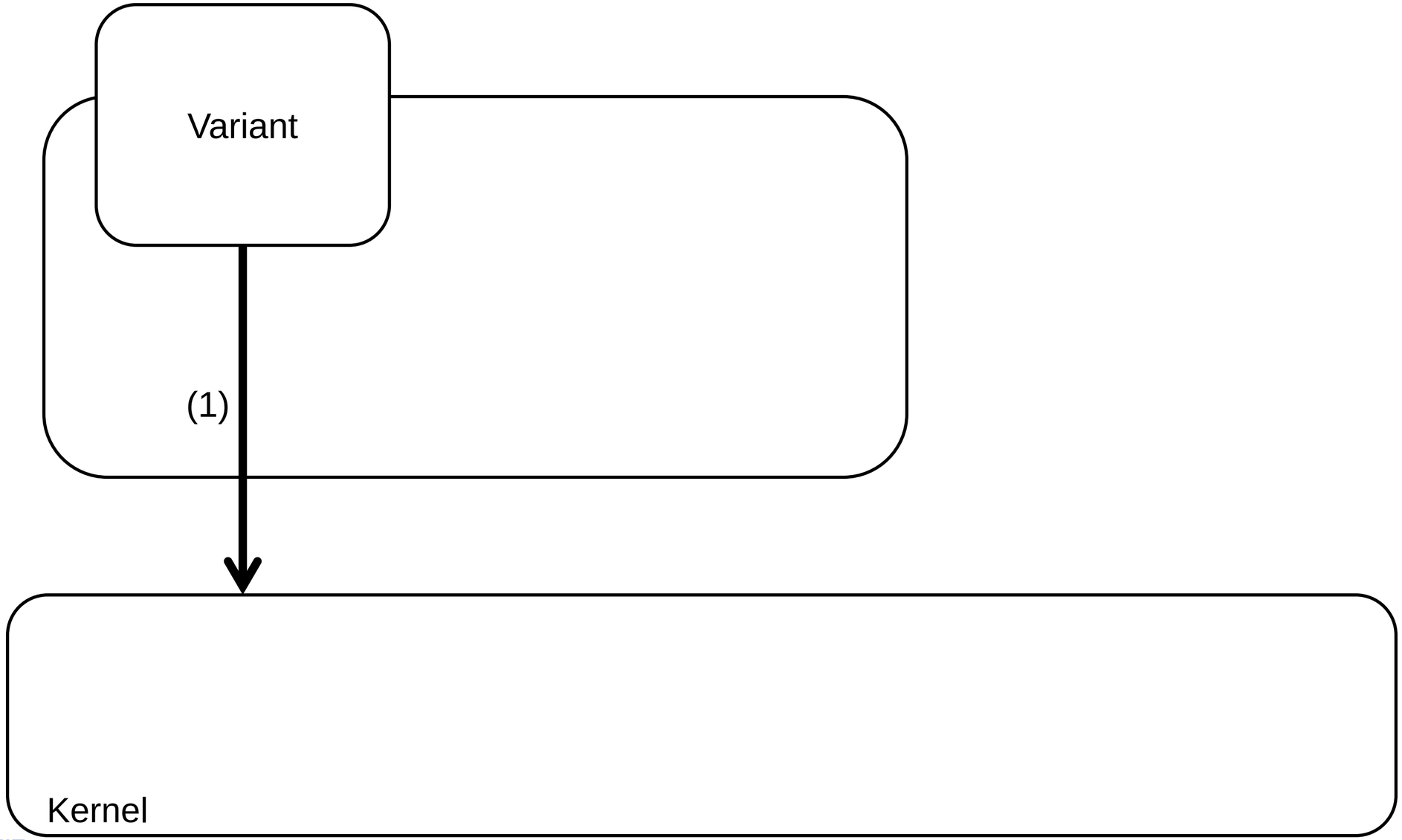
REMON

- Strict Monitoring van veiligheidsgevoelige systeemaanroepen
  - Tracer proces
- Relaxed Monitoring voor niet-veiligheidsgevoelige systeemaanroepen
  - Minder contextswitches

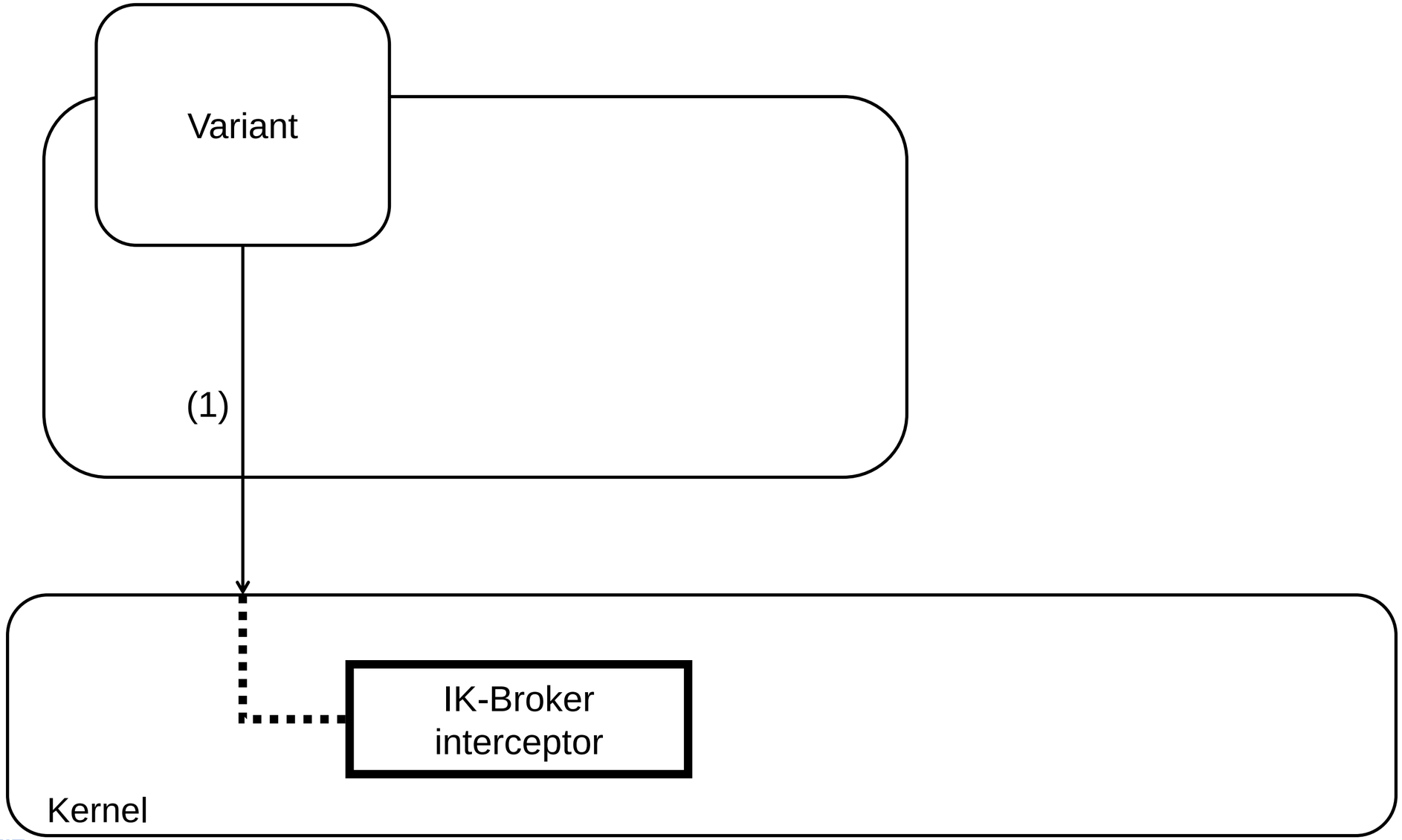
VARIANT VOERT SYSTEM CALLS UIT



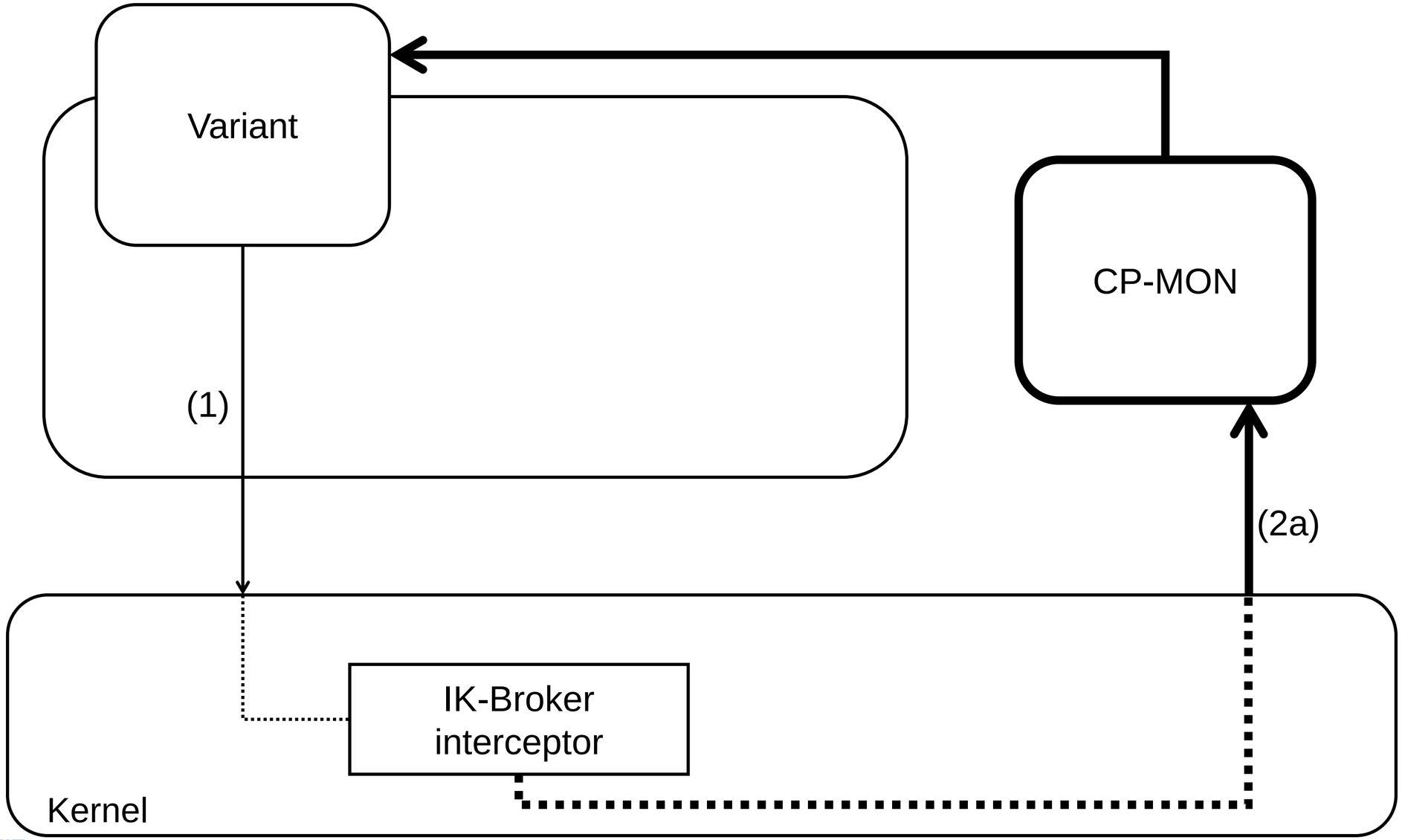
UNIVERSITEIT GENT



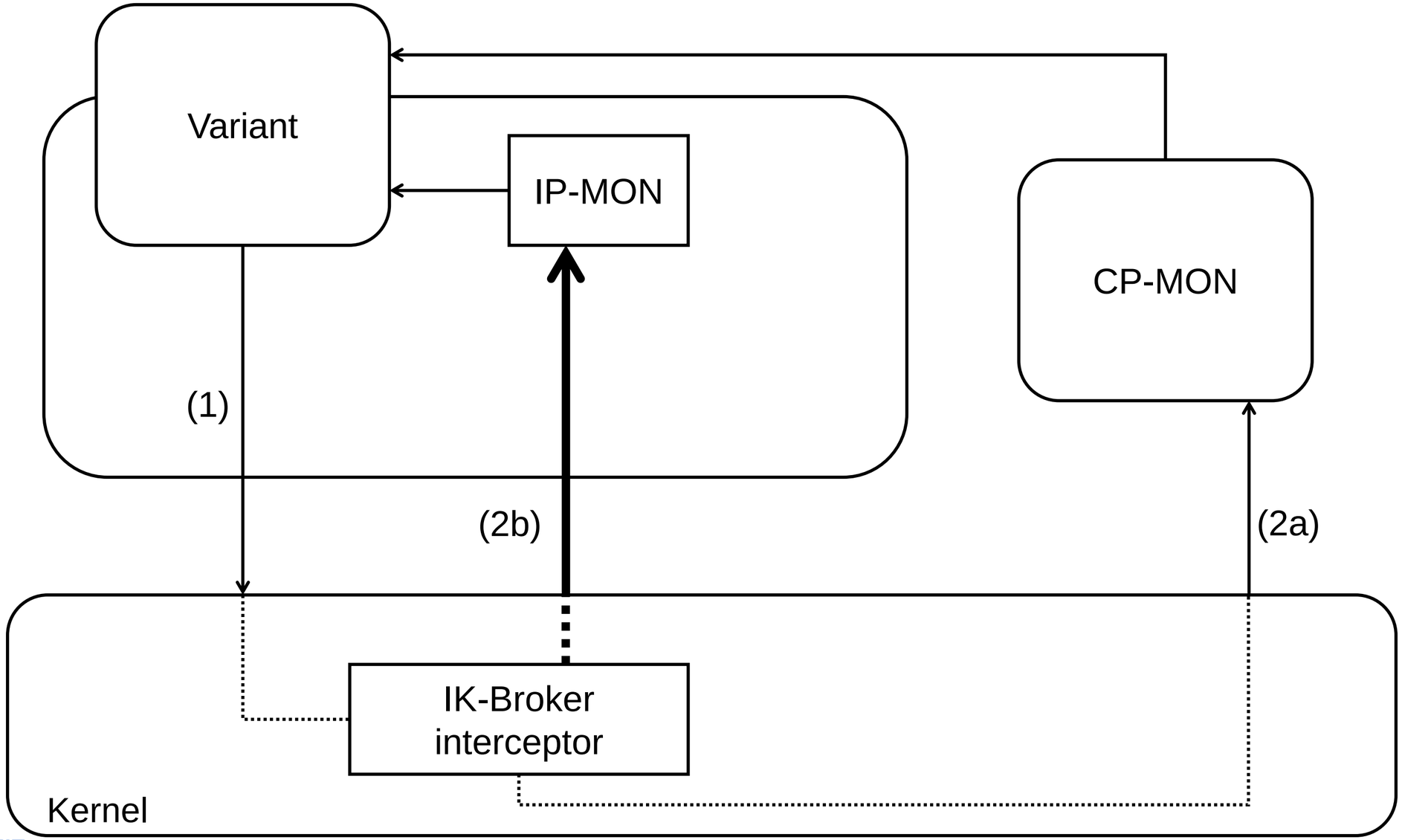
UNIVERSITEIT GENT



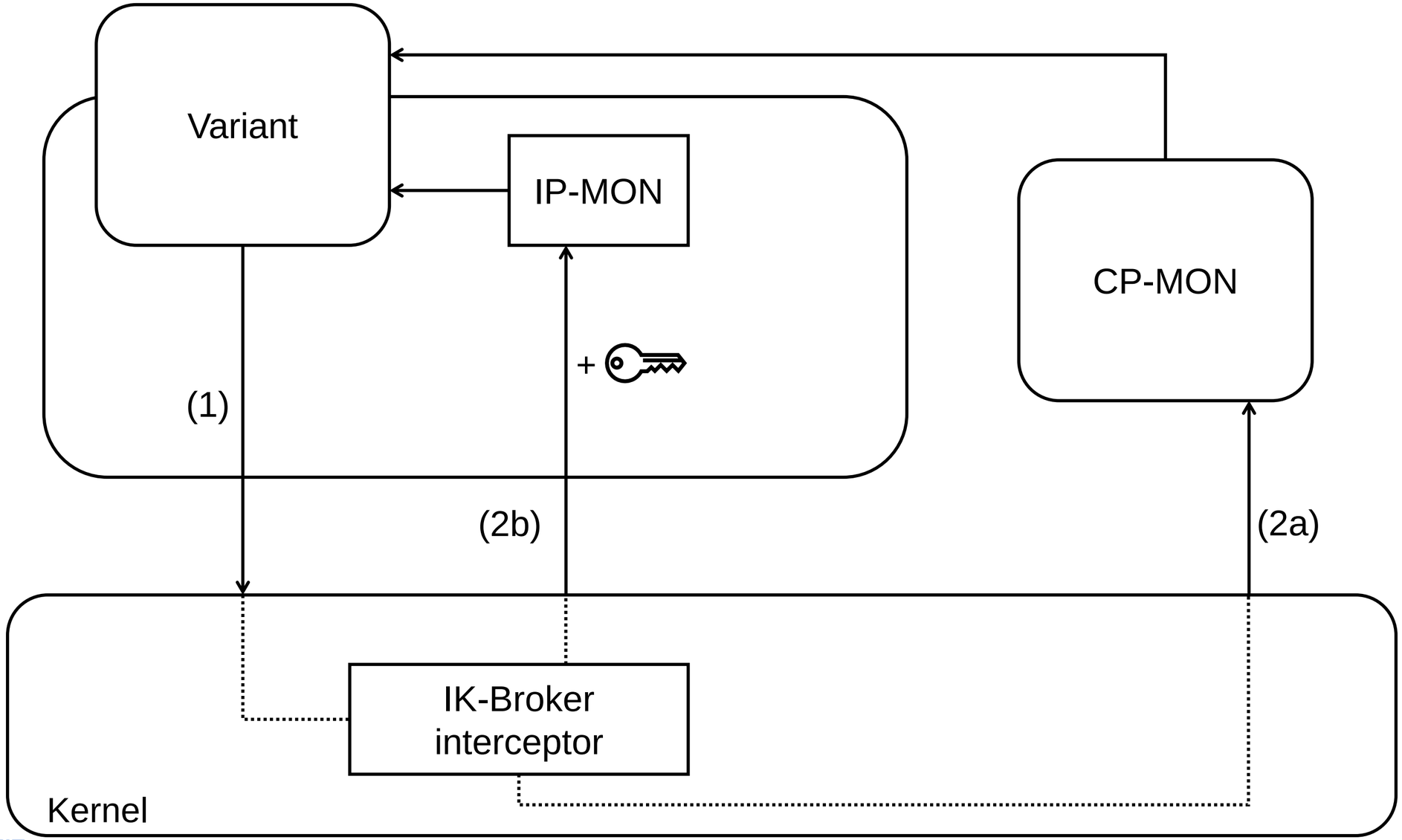
UNIVERSITEIT
GENT



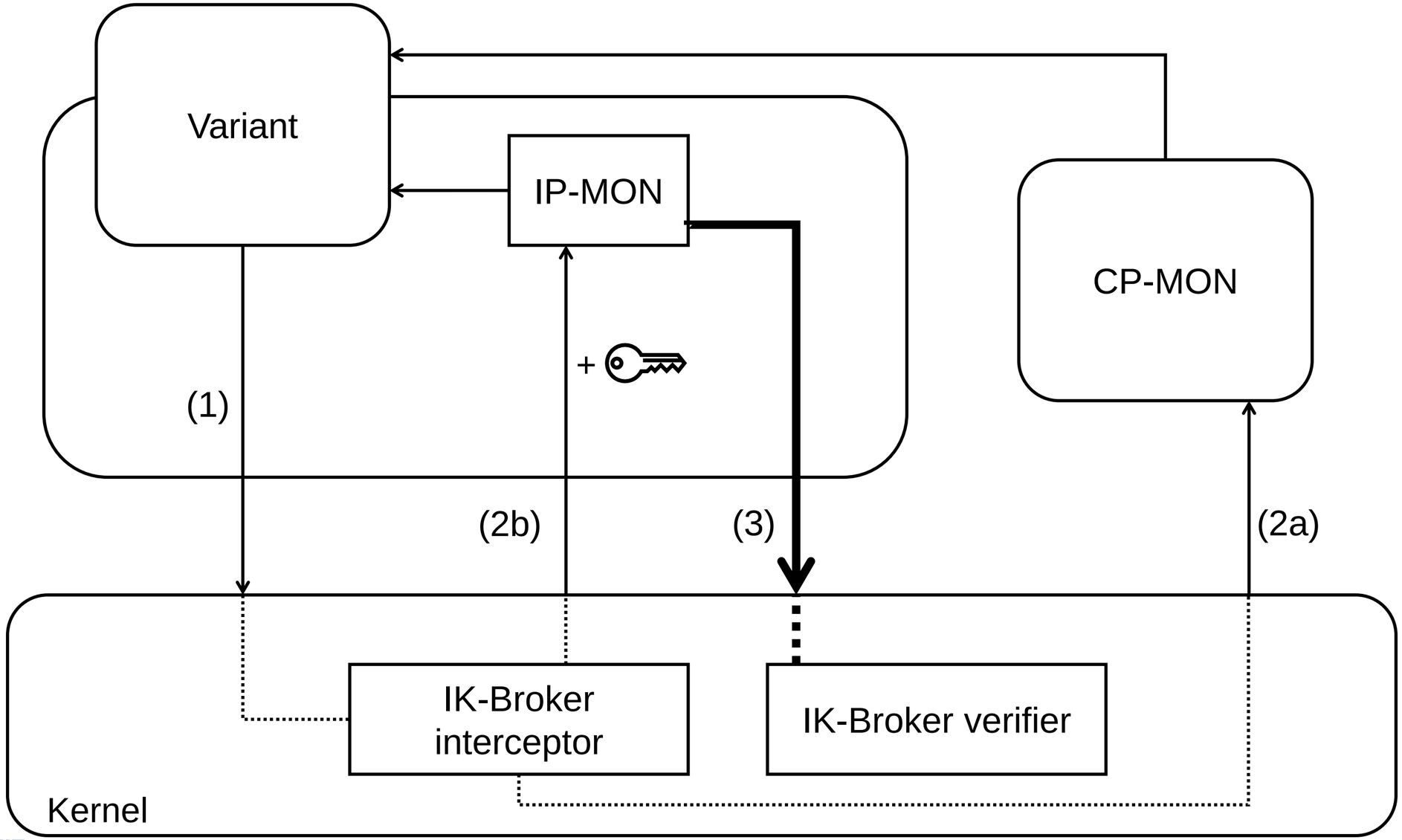
UNIVERSITEIT GENT



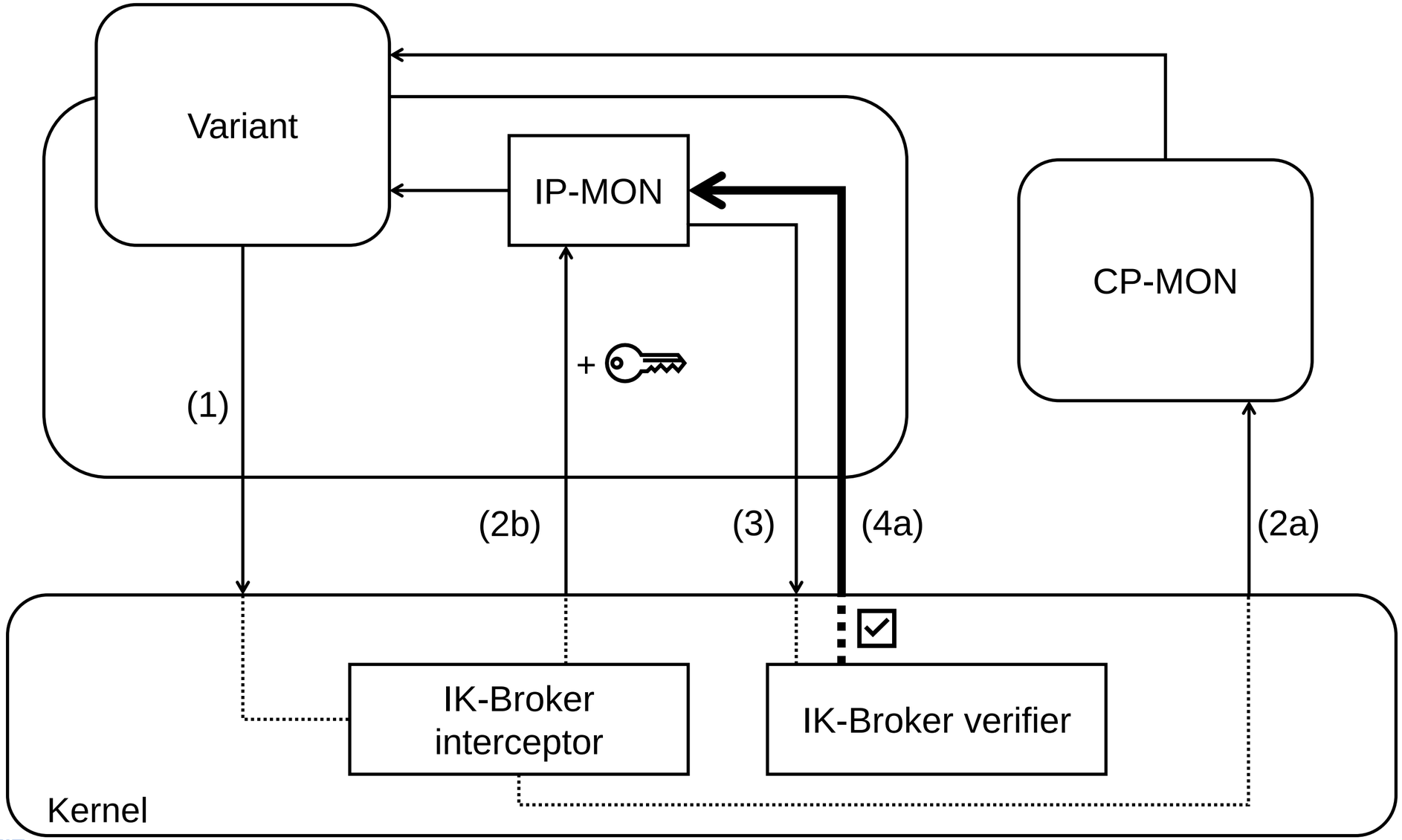
UNIVERSITEIT GENT



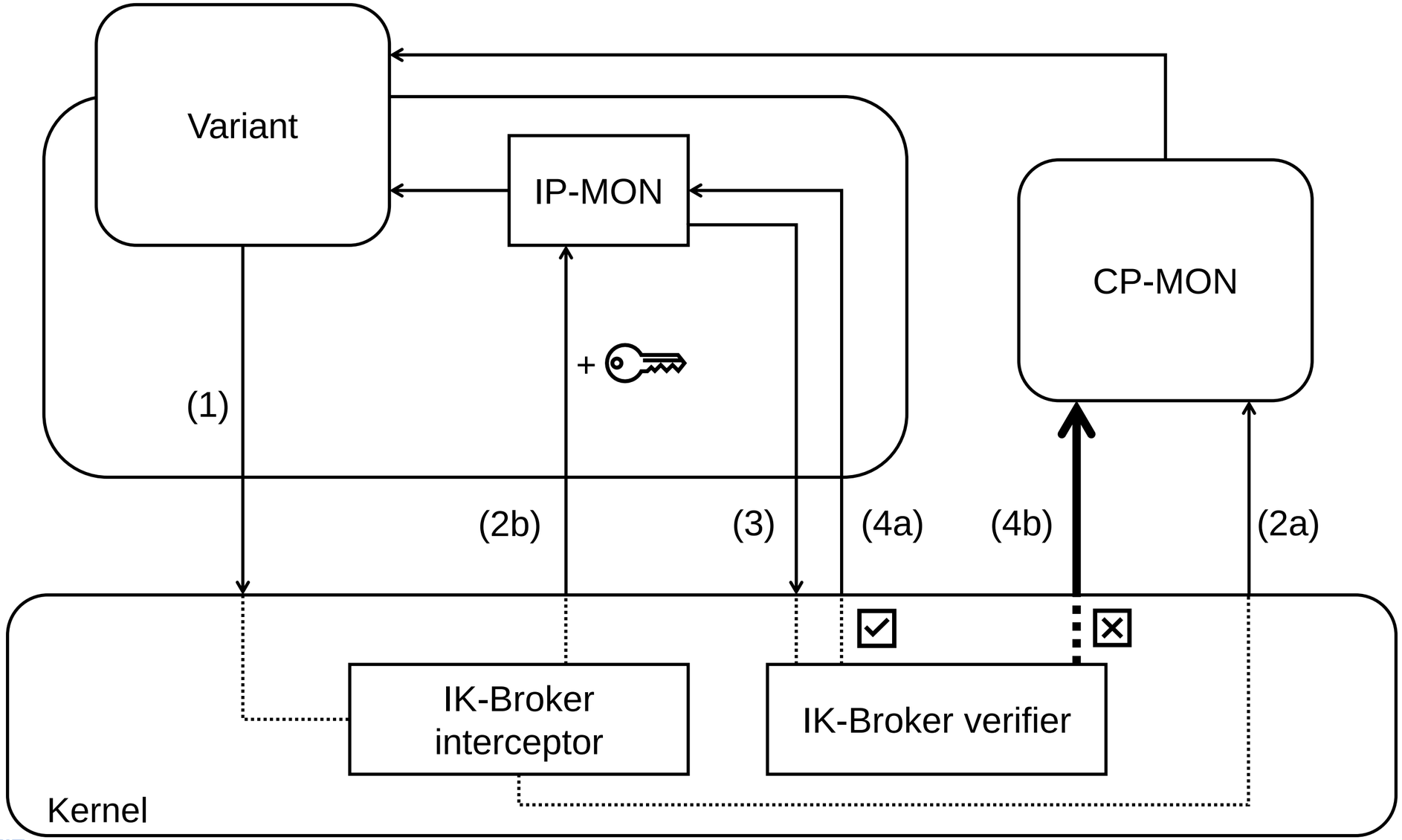
UNIVERSITEIT GENT



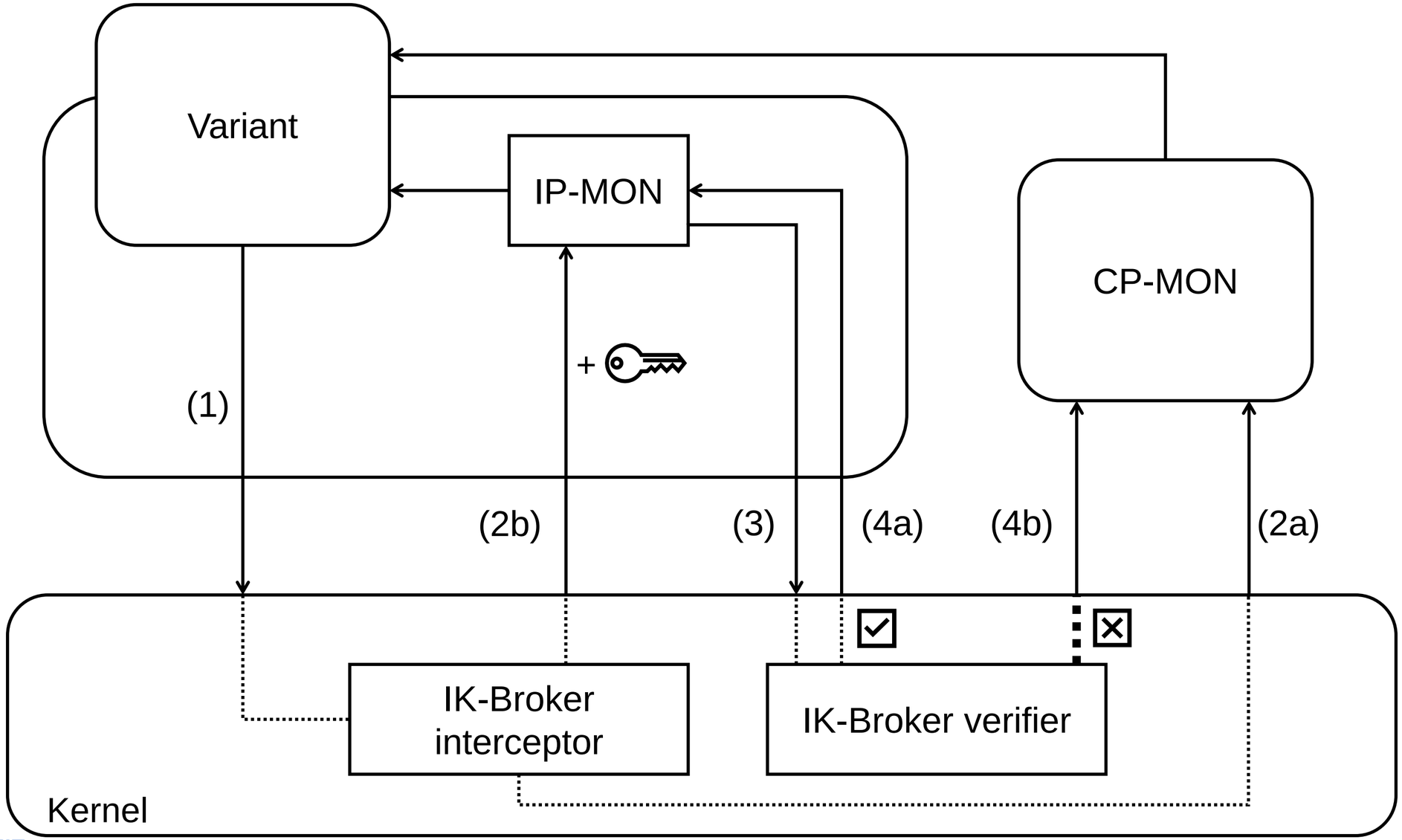
UNIVERSITEIT GENT



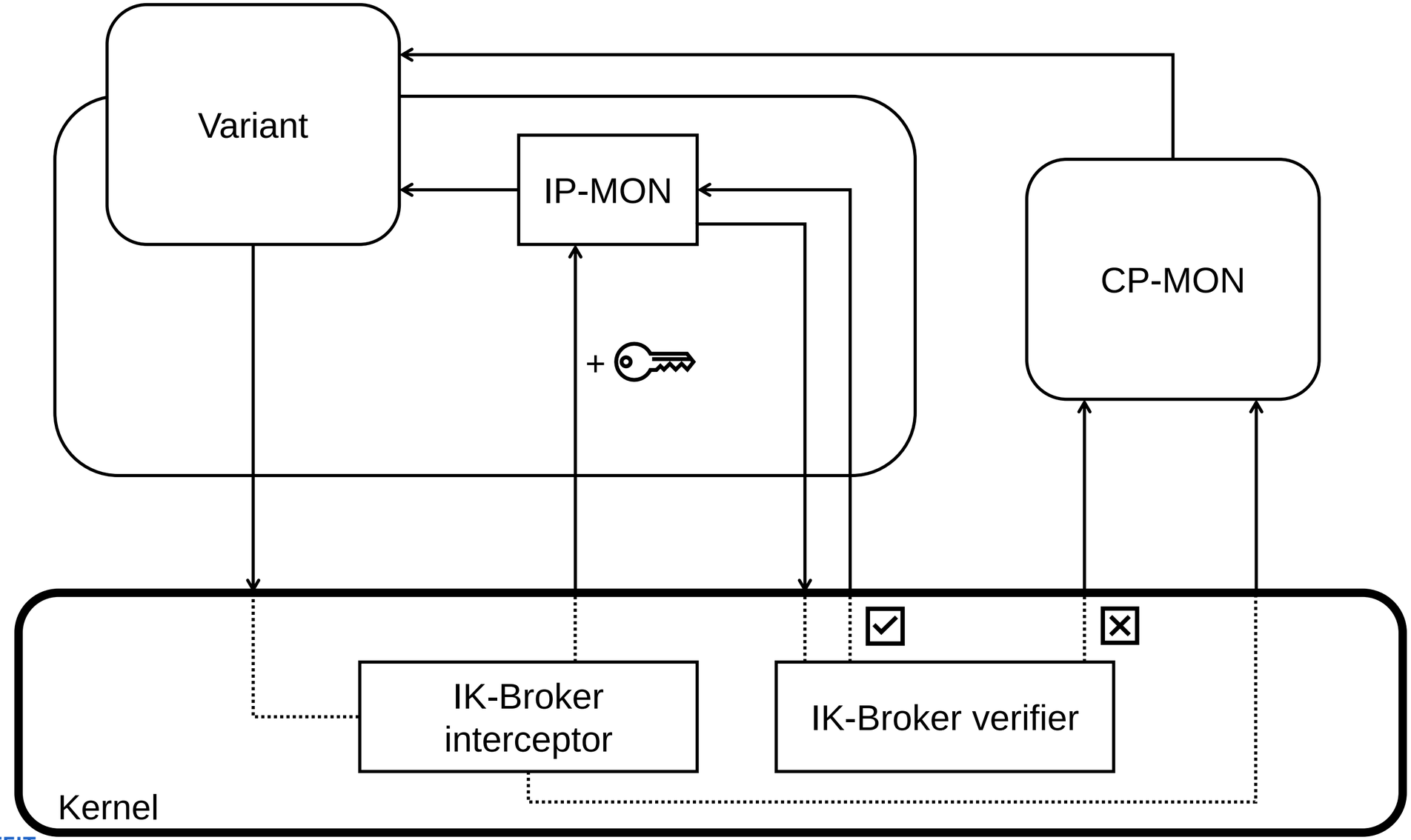
UNIVERSITEIT GENT



UNIVERSITEIT GENT



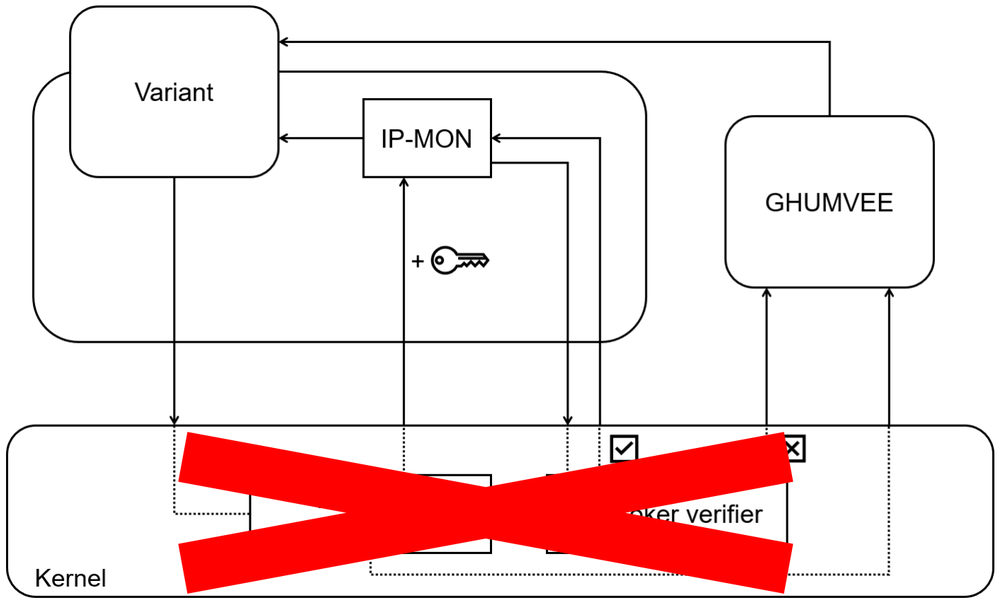
UNIVERSITEIT GENT



UNIVERSITEIT
GENT

DOELSTELLING

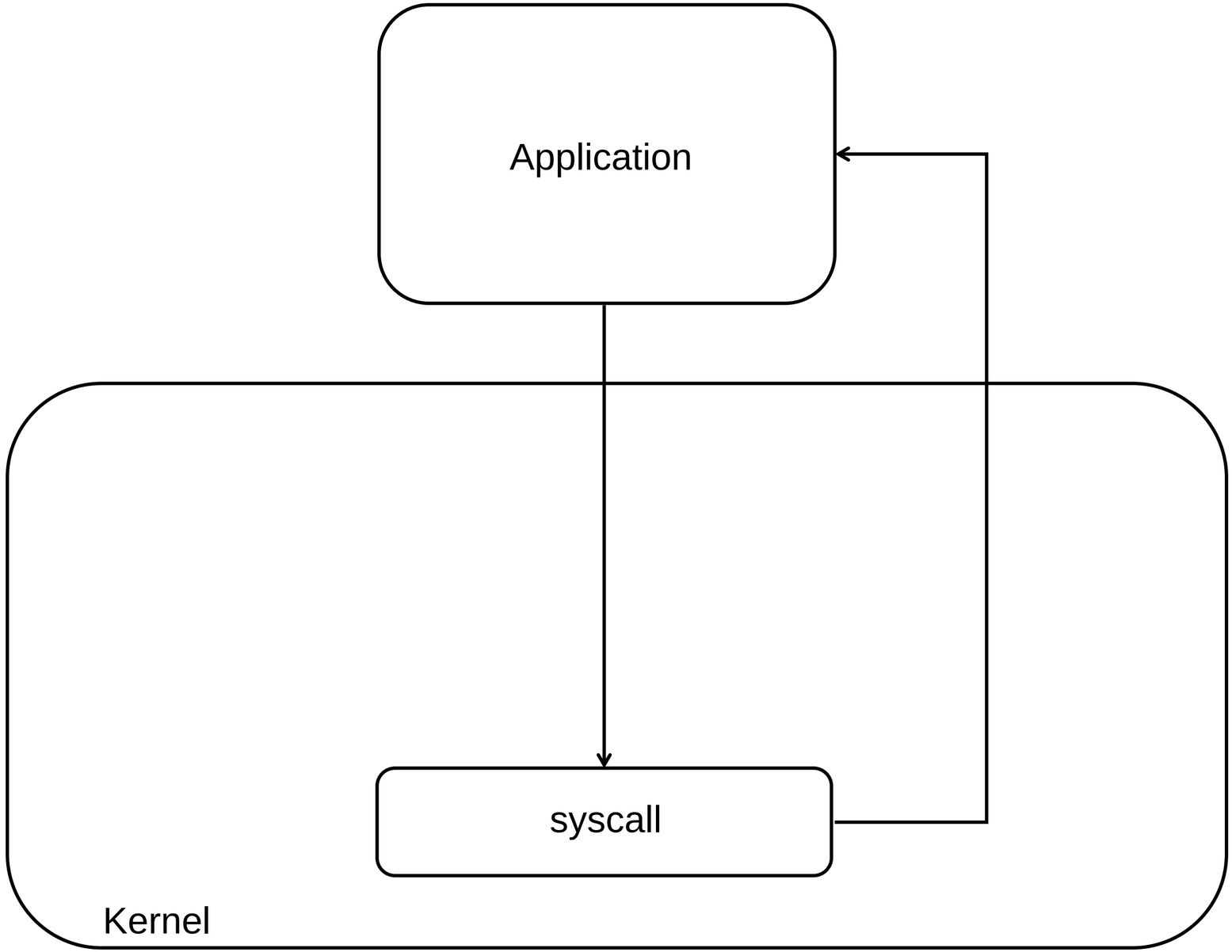
- ReMon aanpassen
  - Kernelpatch vervangen door nieuwe technologieen in de Linux kernel
- Geen verlies van snelheid en veiligheid



UNIVERSITEIT GENT

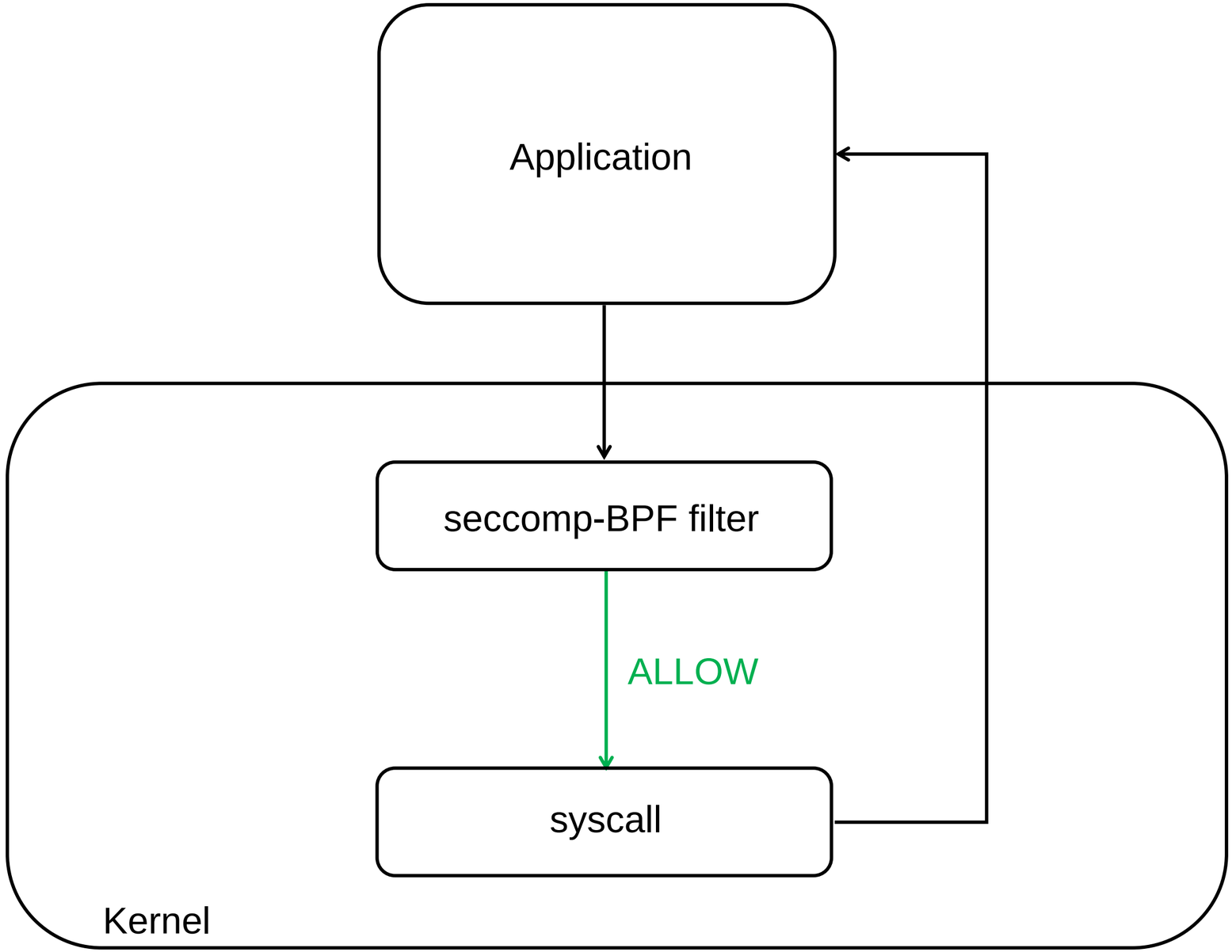
SECCOMP-BPF

SYSTEM CALLS UITVOEREN



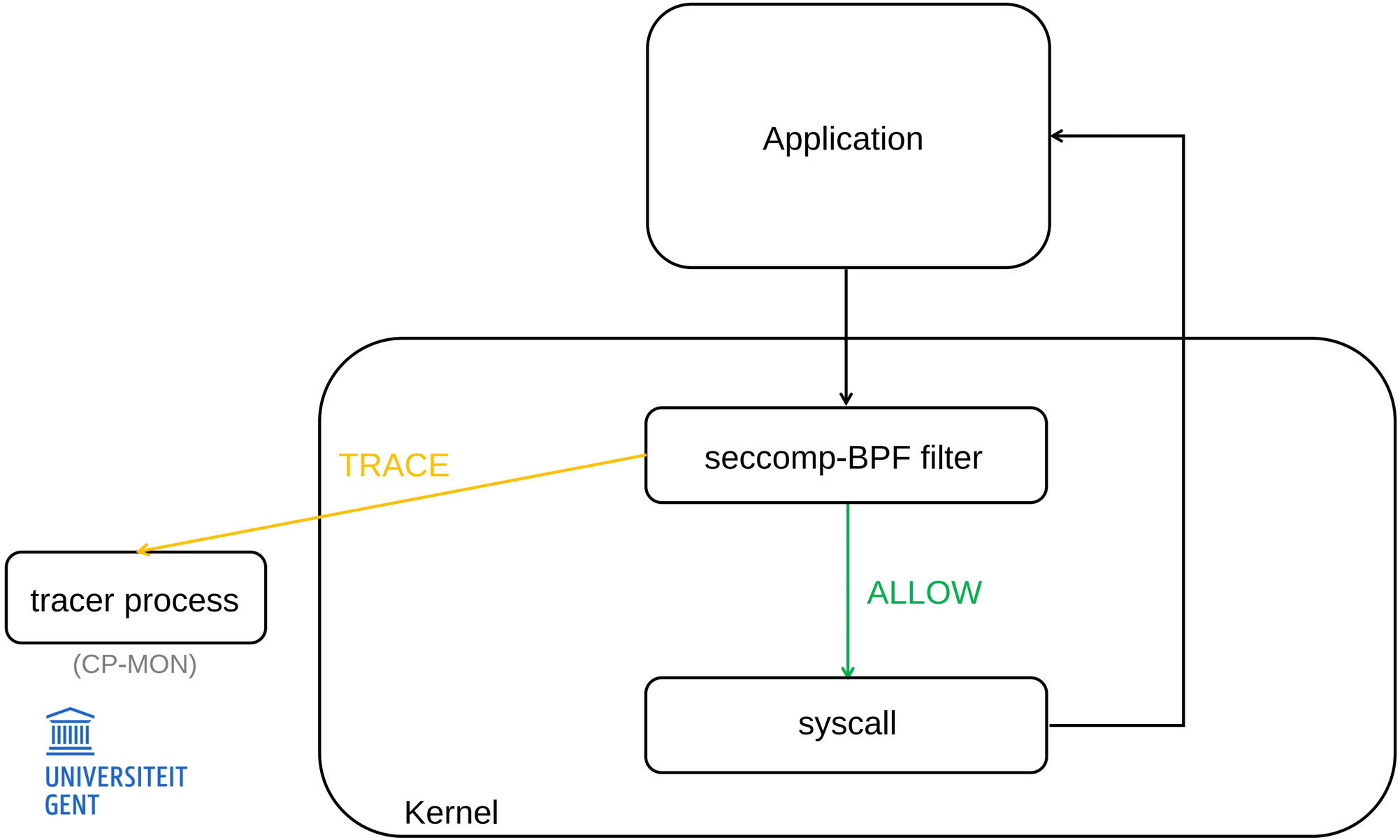
UNIVERSITEIT GENT

SYSTEM CALLS DOORLATEN



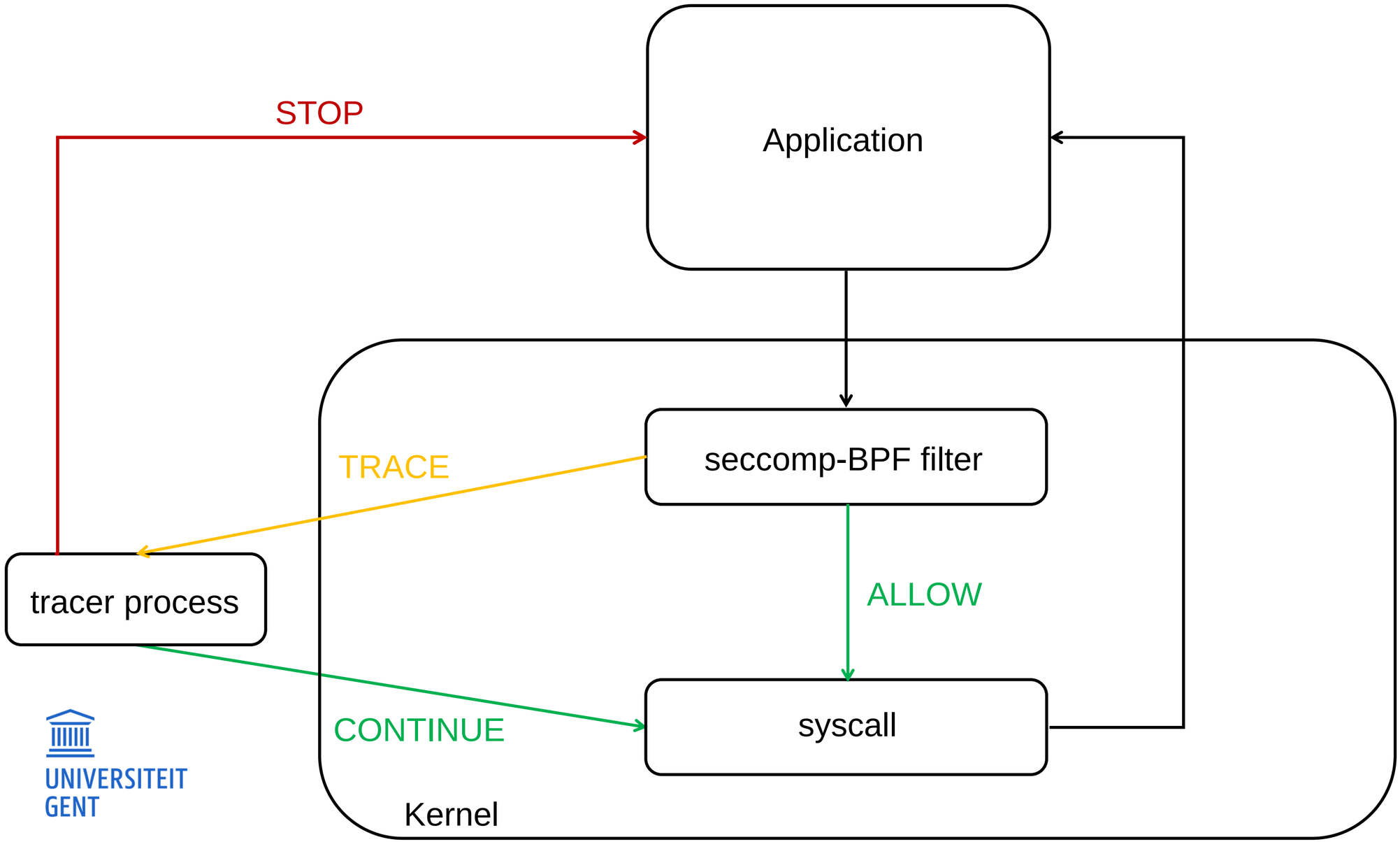
UNIVERSITEIT GENT

SYSTEM CALLS TRACEN



UNIVERSITEIT GENT

HERVATTEN NA SYSTEM CALL TRACE



UNIVERSITEIT GENT

MOGELIJKE ACTIES

- Allow
- Trace
- Errno-waarde terugsturen
  - Systeemaanroep wordt niet uitgevoerd

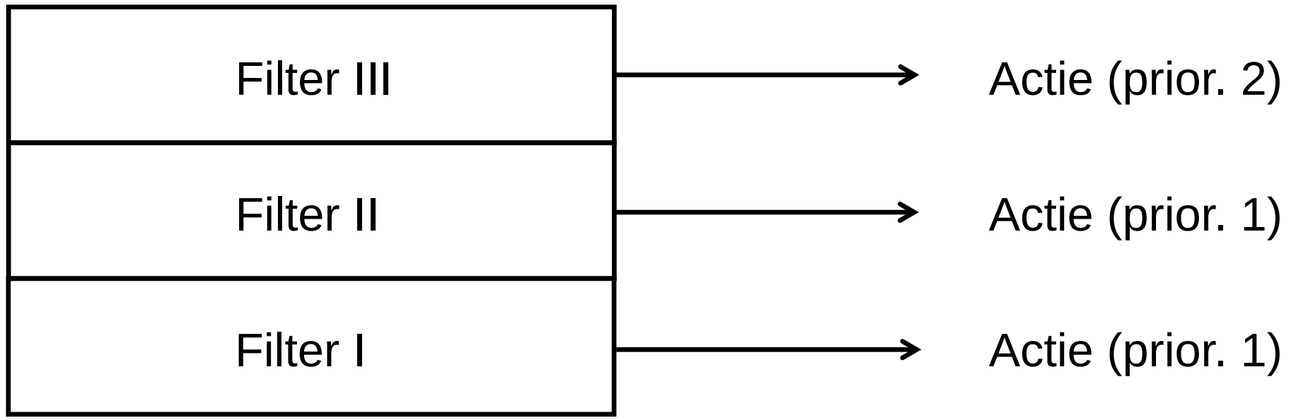
UNIVERSITEIT GENT

MINPUNTEN

- Errno-waarde is 16 bit dat wordt afgetopt op 12 bit

- Elke actie heeft een bepaalde prioriteit
- Combineren van filters voert elke filter uit en geeft actie met hoogste prioriteit terug

} Combineren van filters geeft vaak ongewenst gedrag

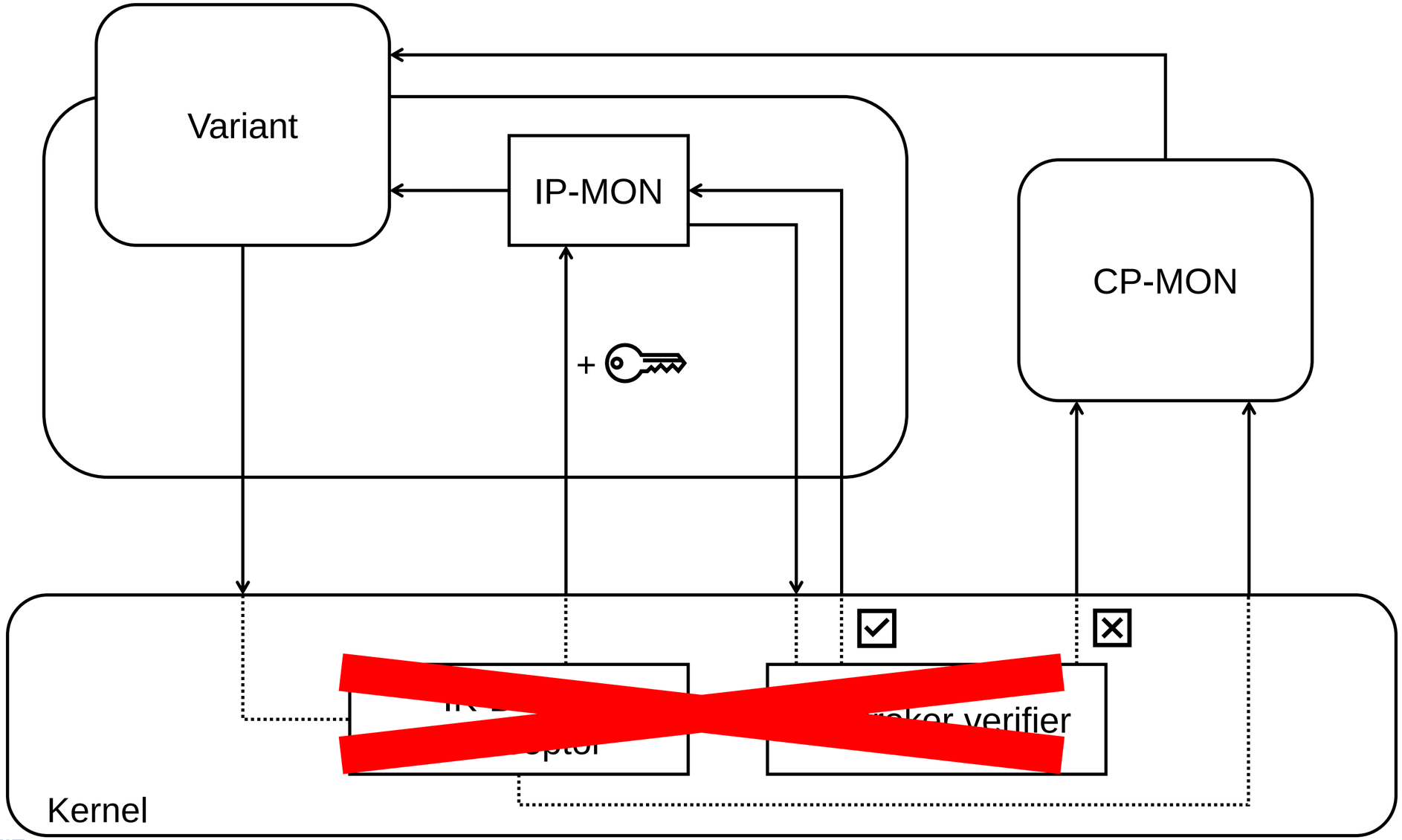


UNIVERSITEIT GENT

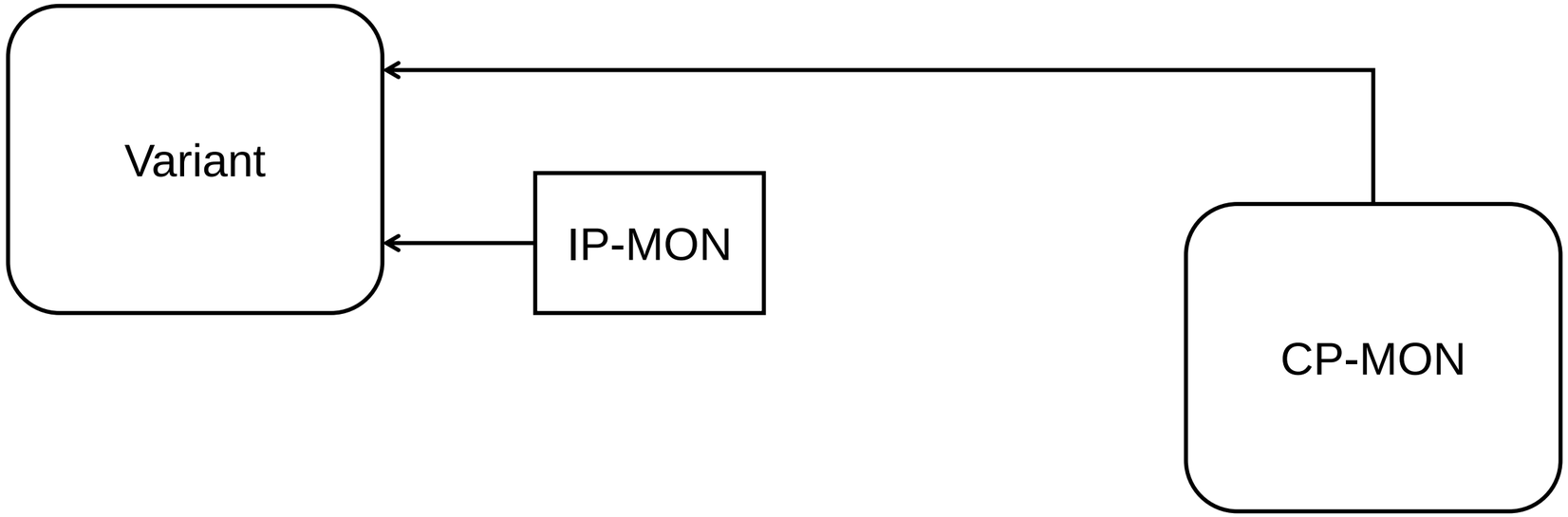
NIEUW DESIGN REMON MET SECCOMP-BPF

UNIVERSITEIT GENT

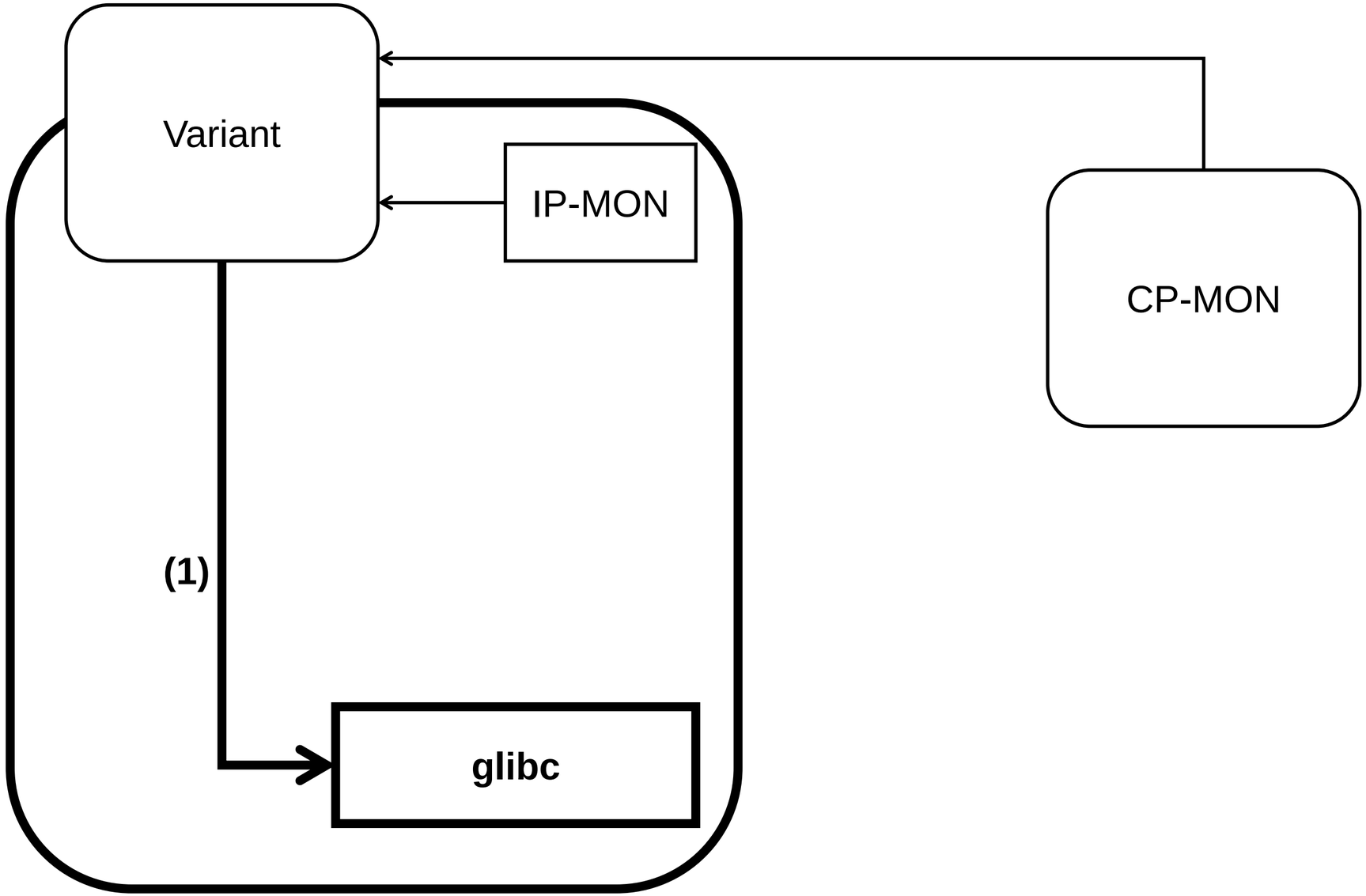
VERVANGEN KERNELPATCH



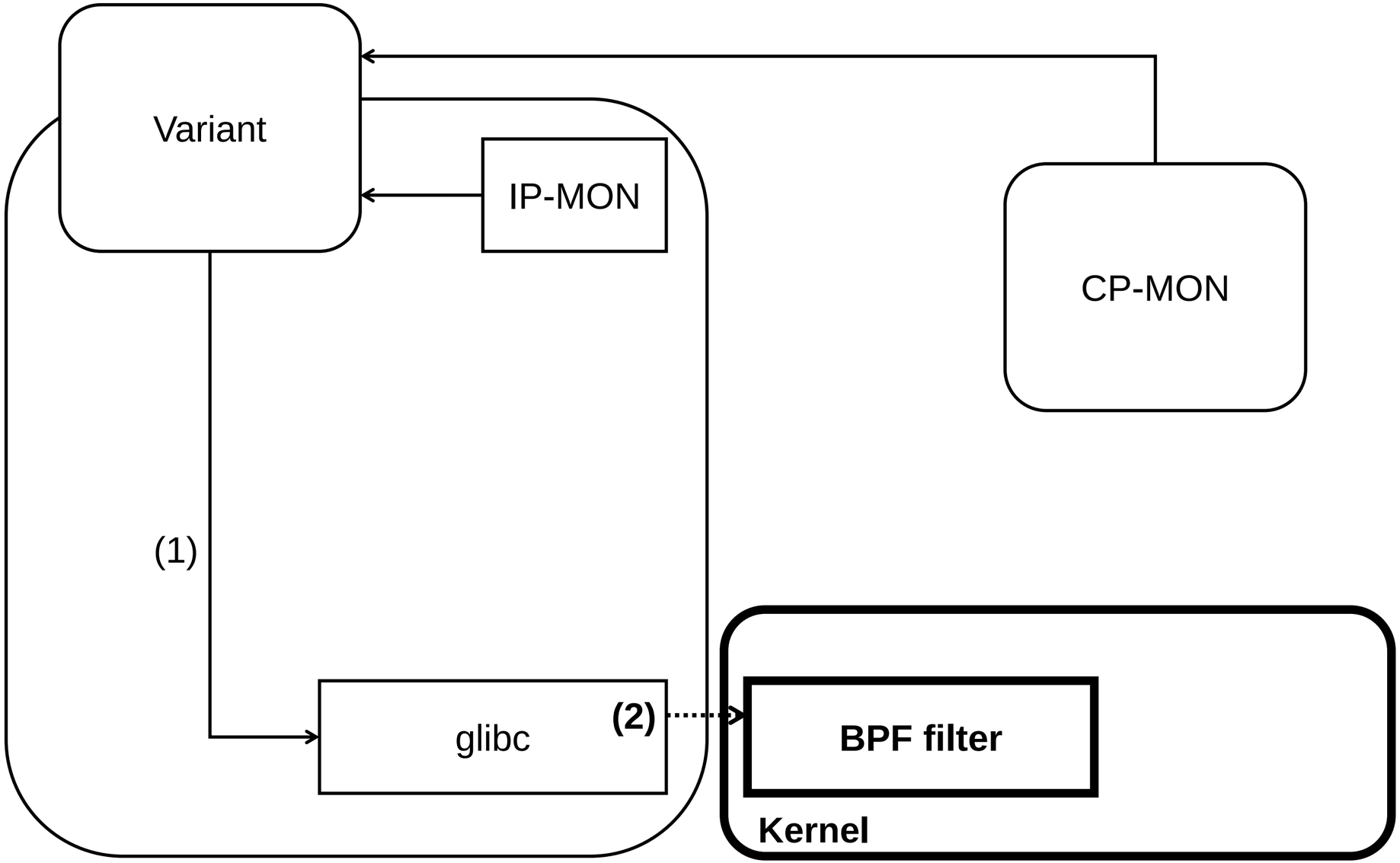
UNIVERSITEIT GENT



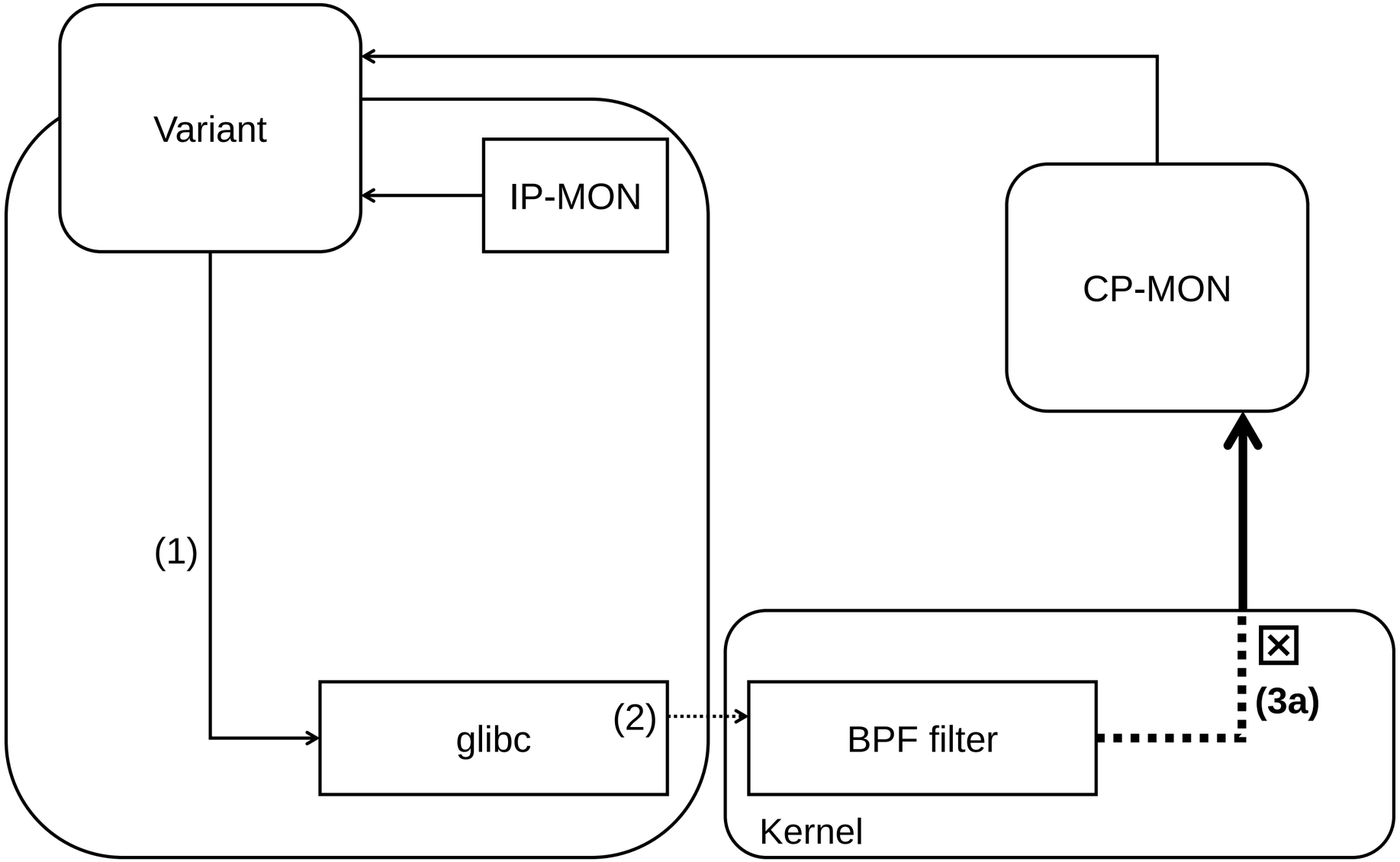
UNIVERSITEIT GENT



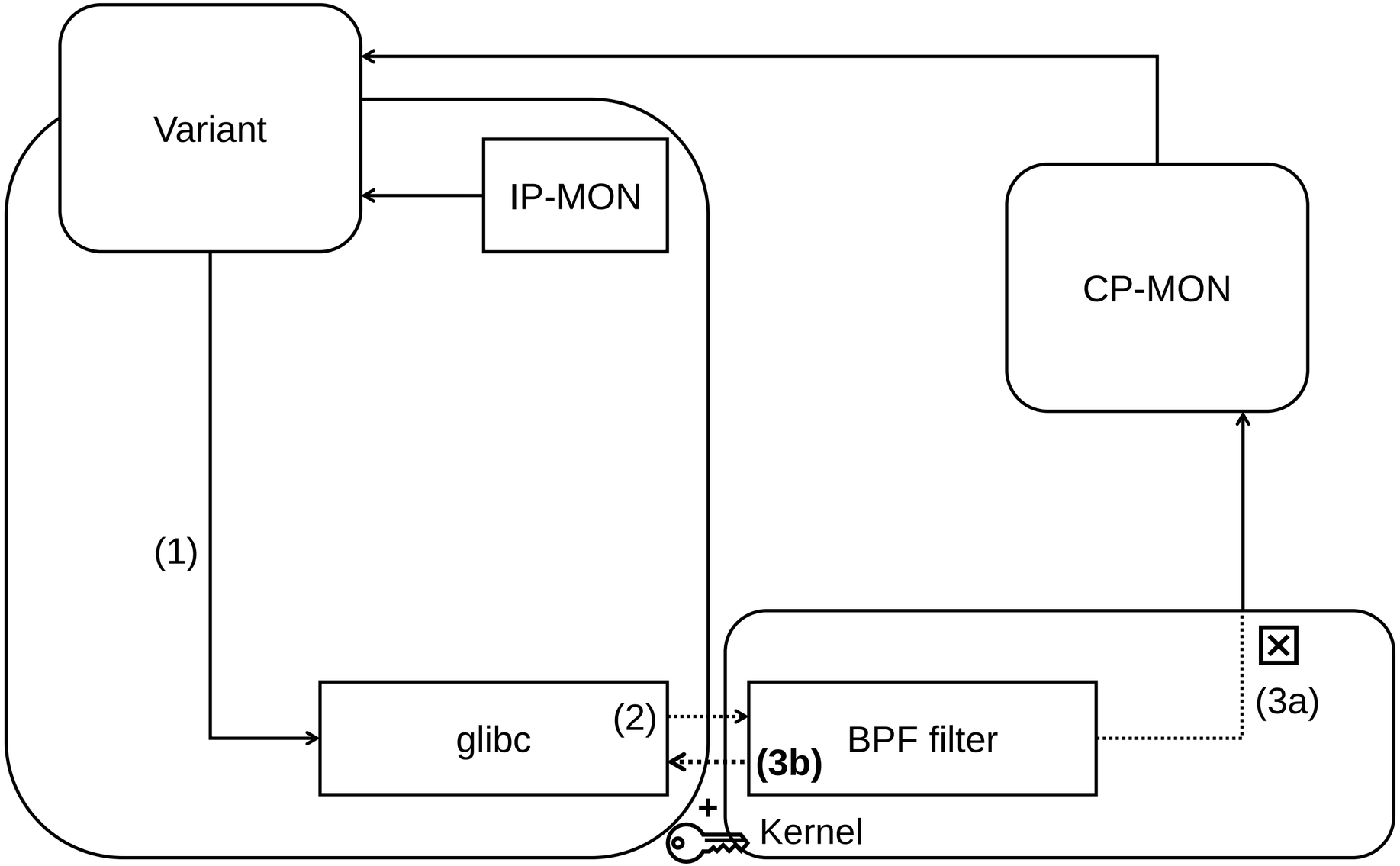
UNIVERSITEIT GENT



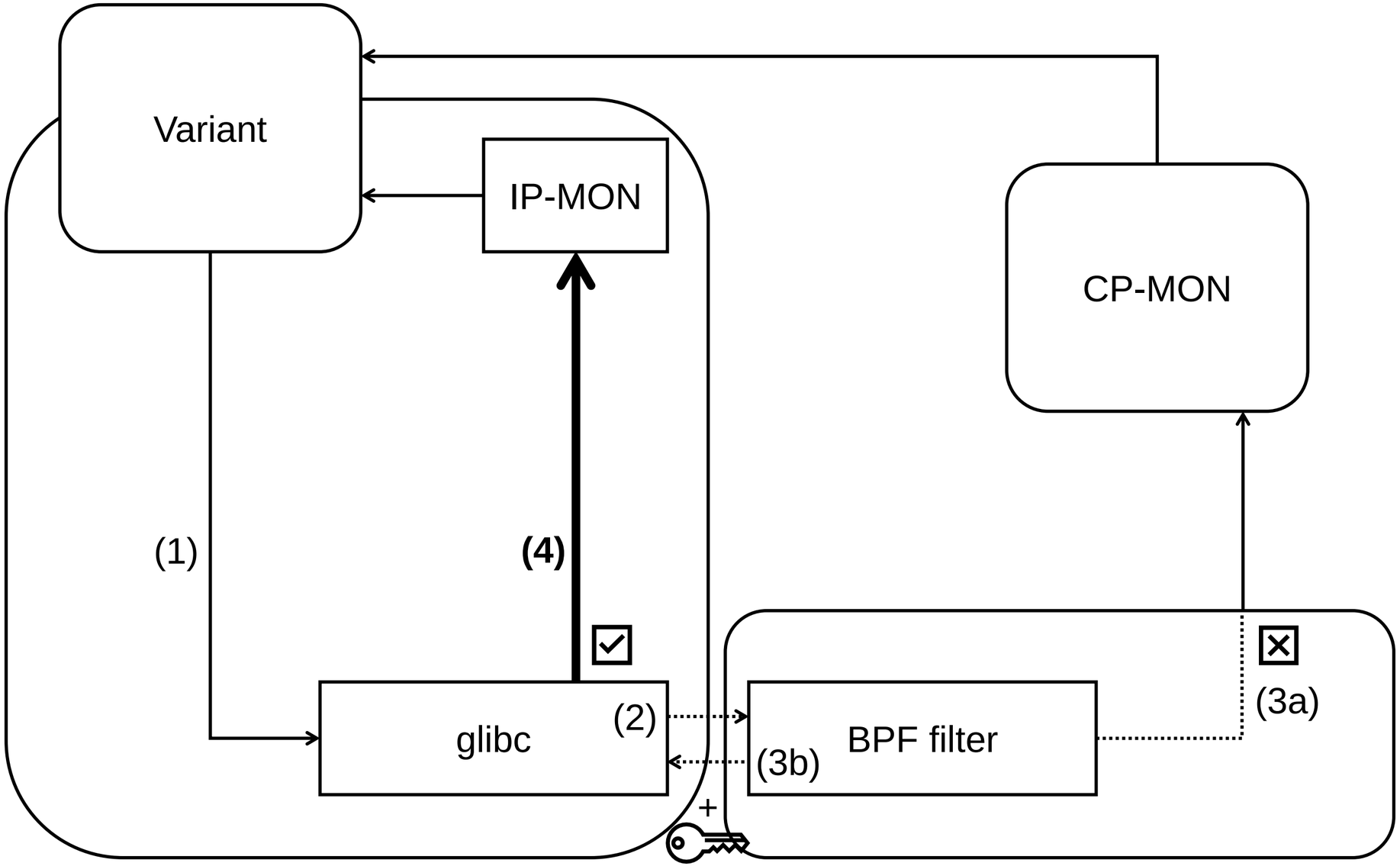
UNIVERSITEIT GENT



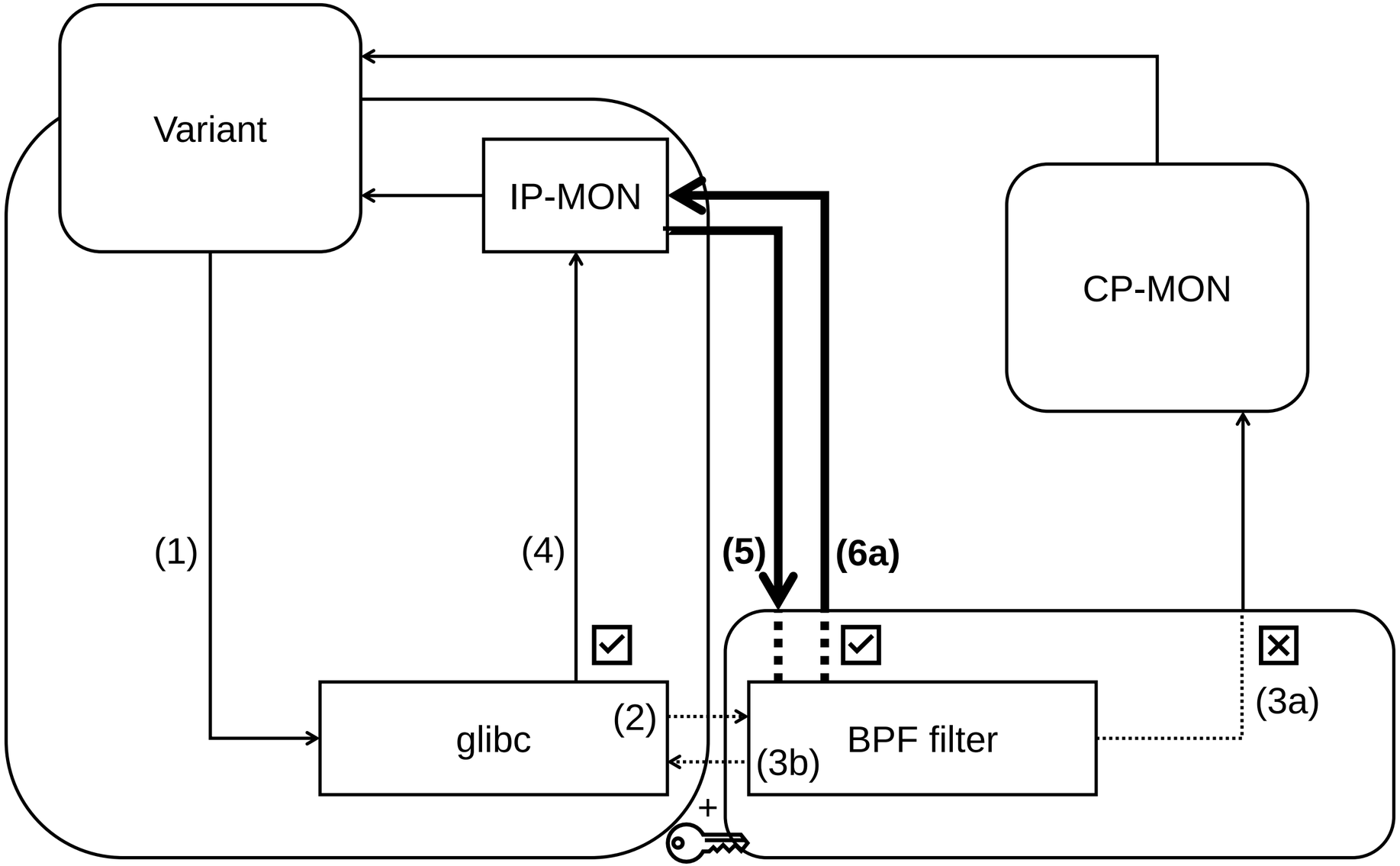
UNIVERSITEIT GENT



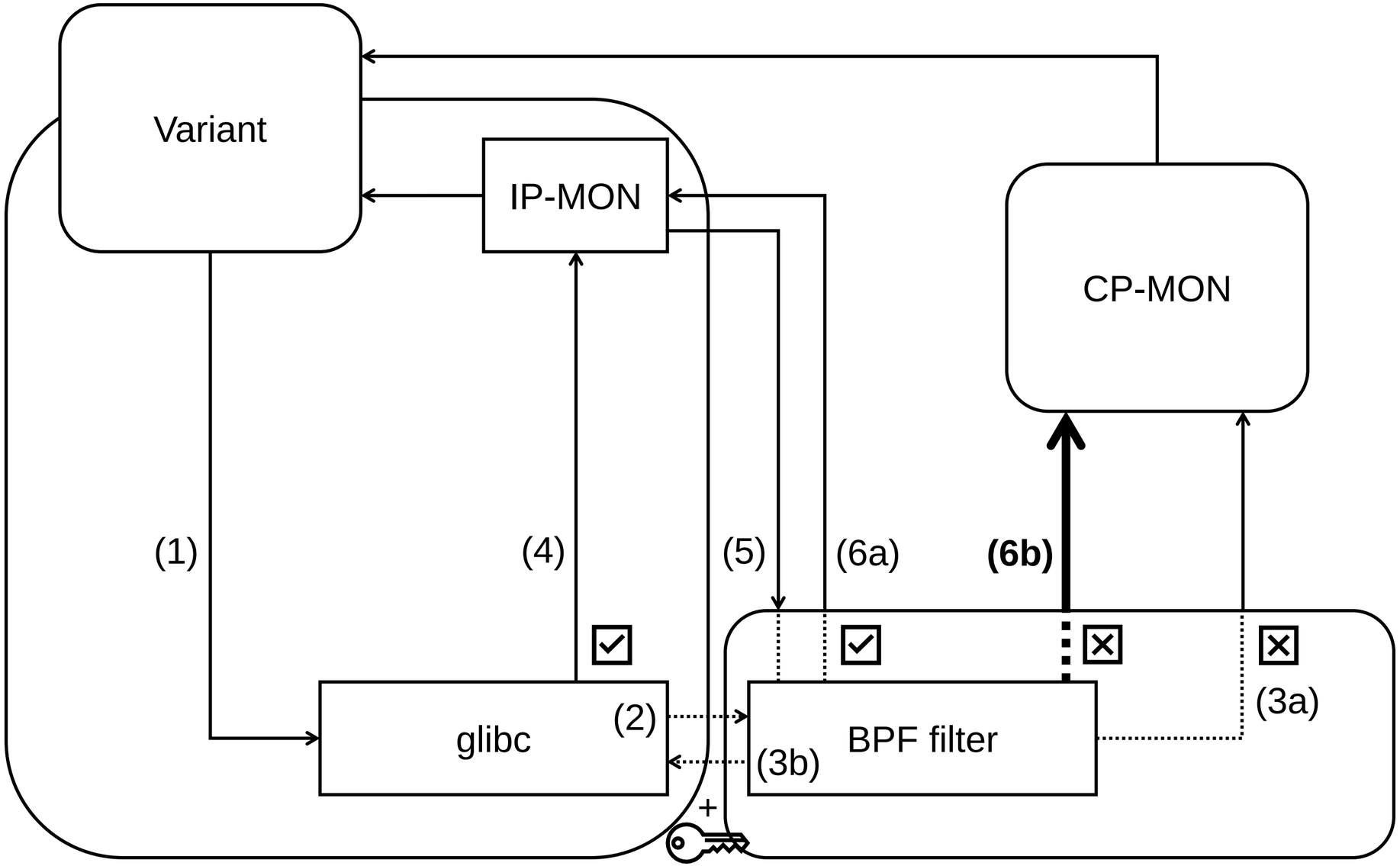
UNIVERSITEIT GENT



UNIVERSITEIT GENT

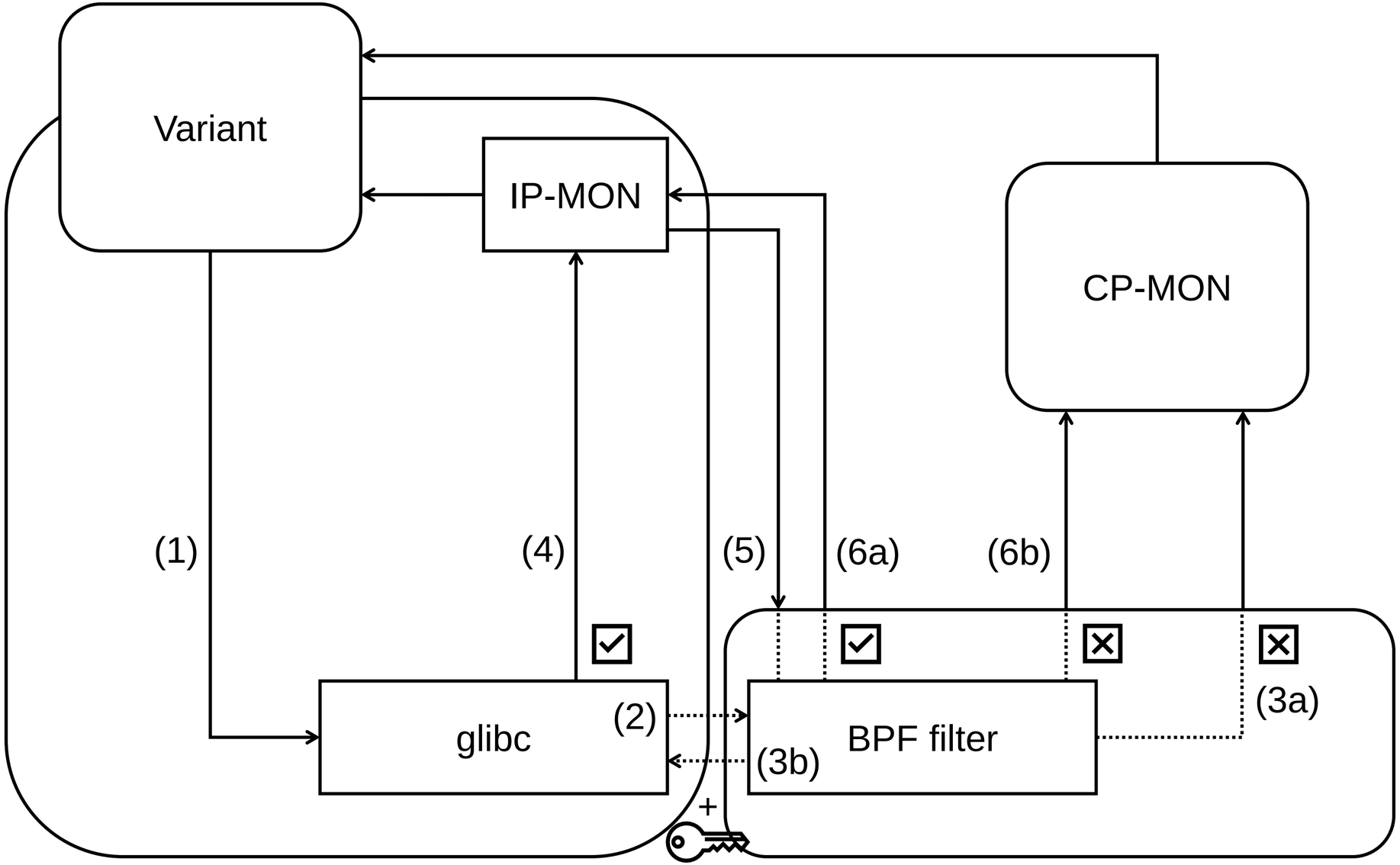


UNIVERSITEIT GENT



UNIVERSITEIT GENT

NIEUW DESIGN



UNIVERSITEIT GENT

VEILIGHEIDSASPECT

UNIVERSITEIT
GENT

GROOTTE VAN SECRET

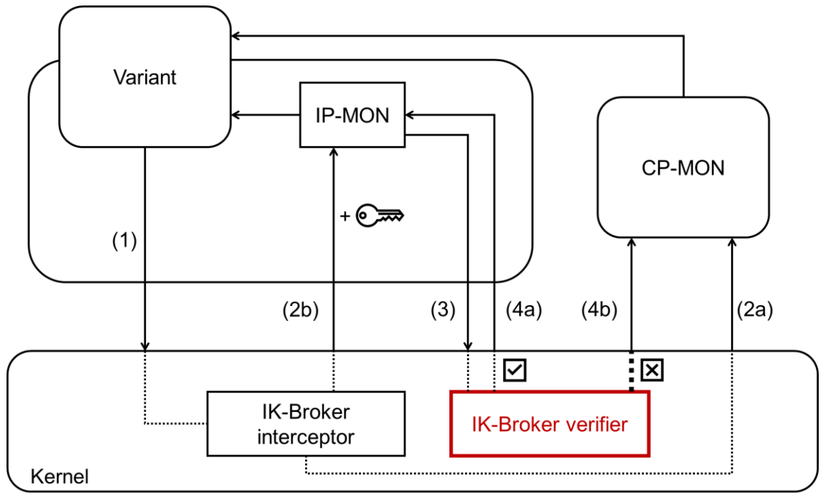
- 12 bit per passage in seccomp-BPF filter
- Meerdere keren passeren in filter
  - 4 keer voor 48 bit

UNIVERSITEIT GENT

VEILIGHEIDSASPECT EERSTE SECRET

Originele IP-MON

- Kernel geeft unieke secret per systeemaanroep van 64 bit
- Random waarde voor controle in broker verifier



IP-MON met Seccomp-BPF

- Niet meer aanwezig
- Geen unieke secret per systeemaanroep mogelijk
- seccomp-BPF filter is constant
- We kunnen controleren van waar de systeemaanroep komt, geen secret nodig

UNIVERSITEIT GENT

VEILIGHEIDSASPECT TWEEDE SECRET

Originele IP-MON

- Unieke 64 bit secret per variant
- Adres van IP-MON

IP-MON met Seccomp-BPF

- Unieke secret per variant
- Adres van IP-MON
- Bij lekken van secret moet de systeemaanroep alsnog via de seccomp-BPF filter passeren voor controle

UNIVERSITEIT GENT

TEKORTKOMINGEN

UNIVERSITEIT
GENT

TEKORTKOMINGEN

- Beperkte set ondersteunde systeemaanroepen in nieuwe versie IP-MON

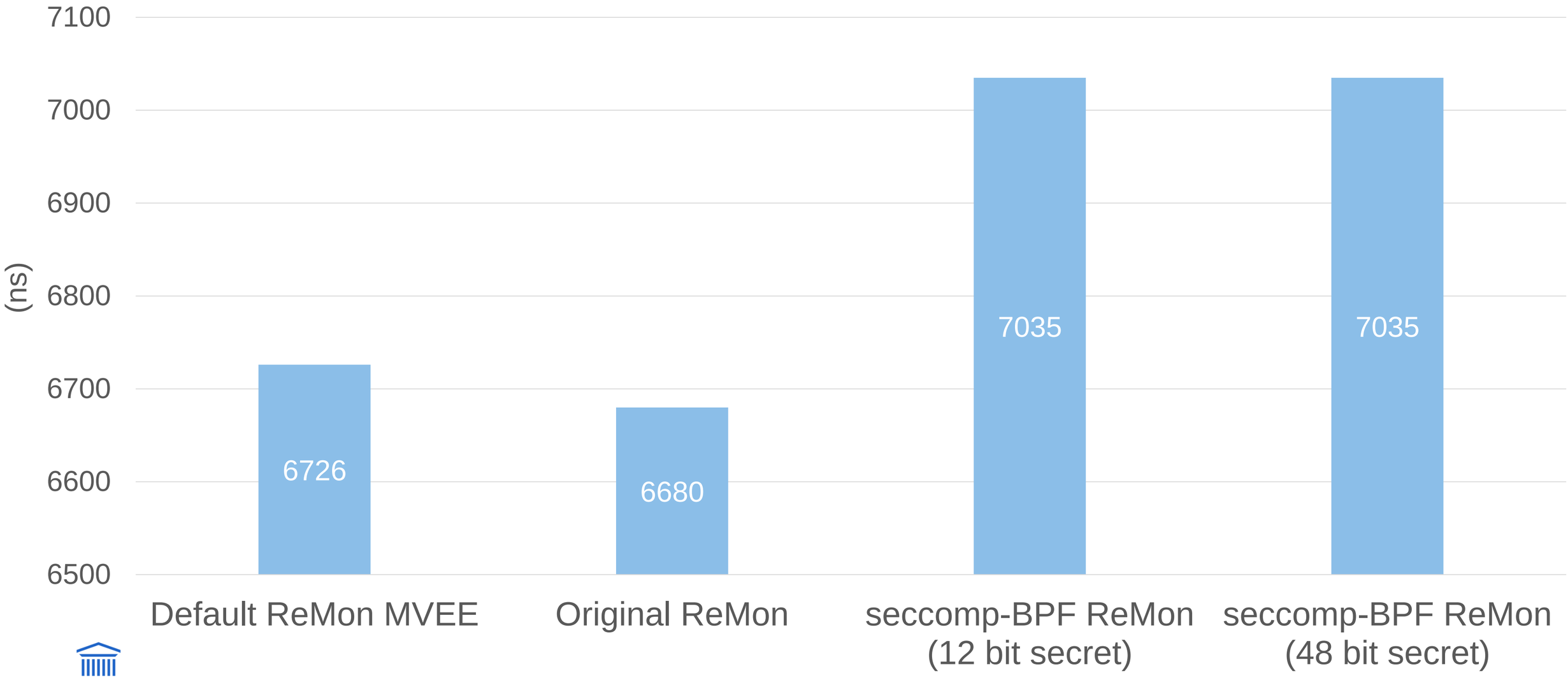
TESTRESULTATEN

UNIVERSITEIT
GENT

MICROBENCHMARK

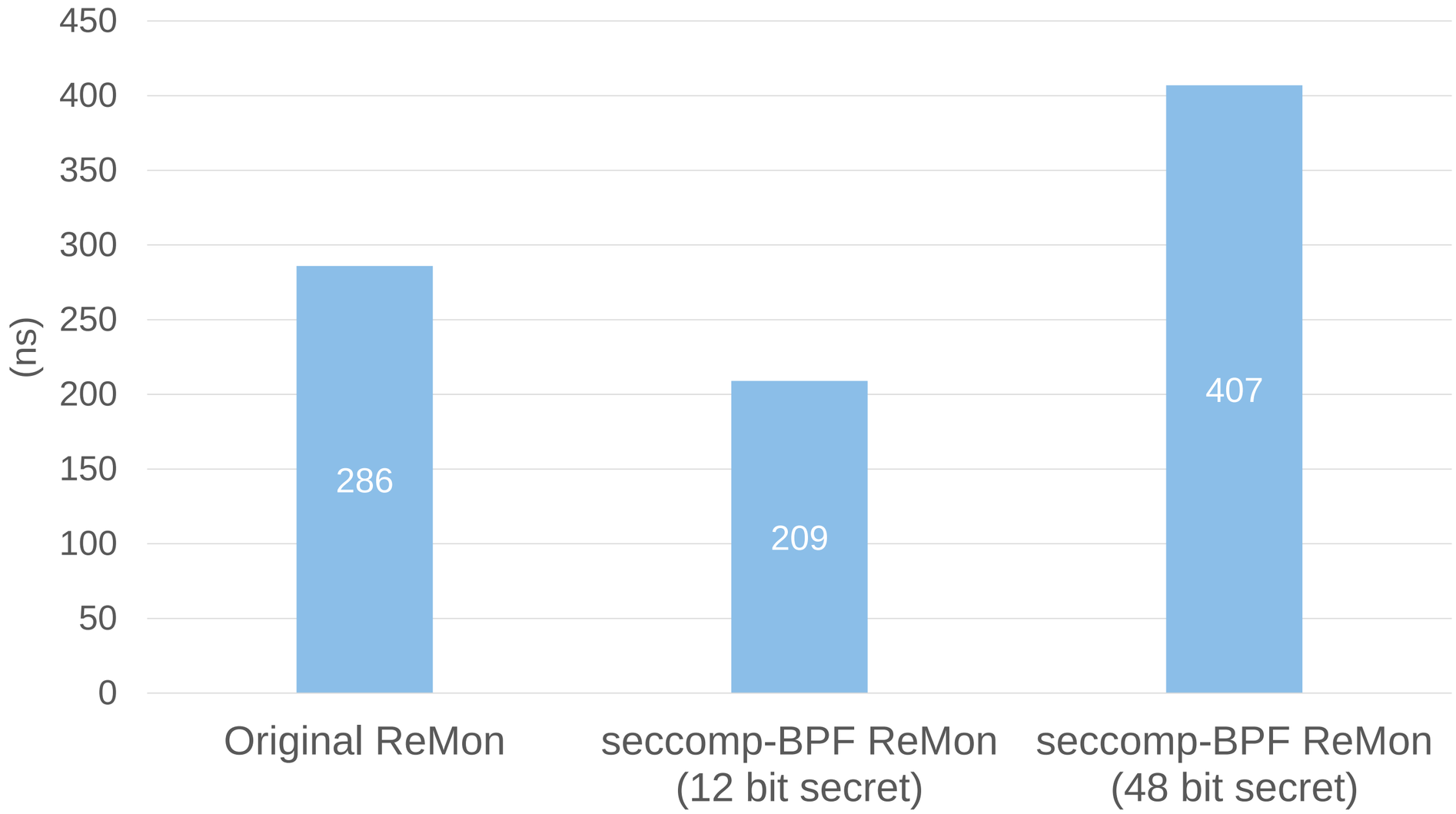
- 5 000 000 getpid()-oproepen die elk een syscall aanroepen
- Resultaat is het gemiddelde van de uitvoeringstijd van 1 getpid() over verschillende runs
- Overhead van Seccomp-BPF meten

RESULTATEN – ALLES NAAR CP-MON



UNIVERSITEIT GENT

RESULTATEN – GETPID NAAR IP-MON



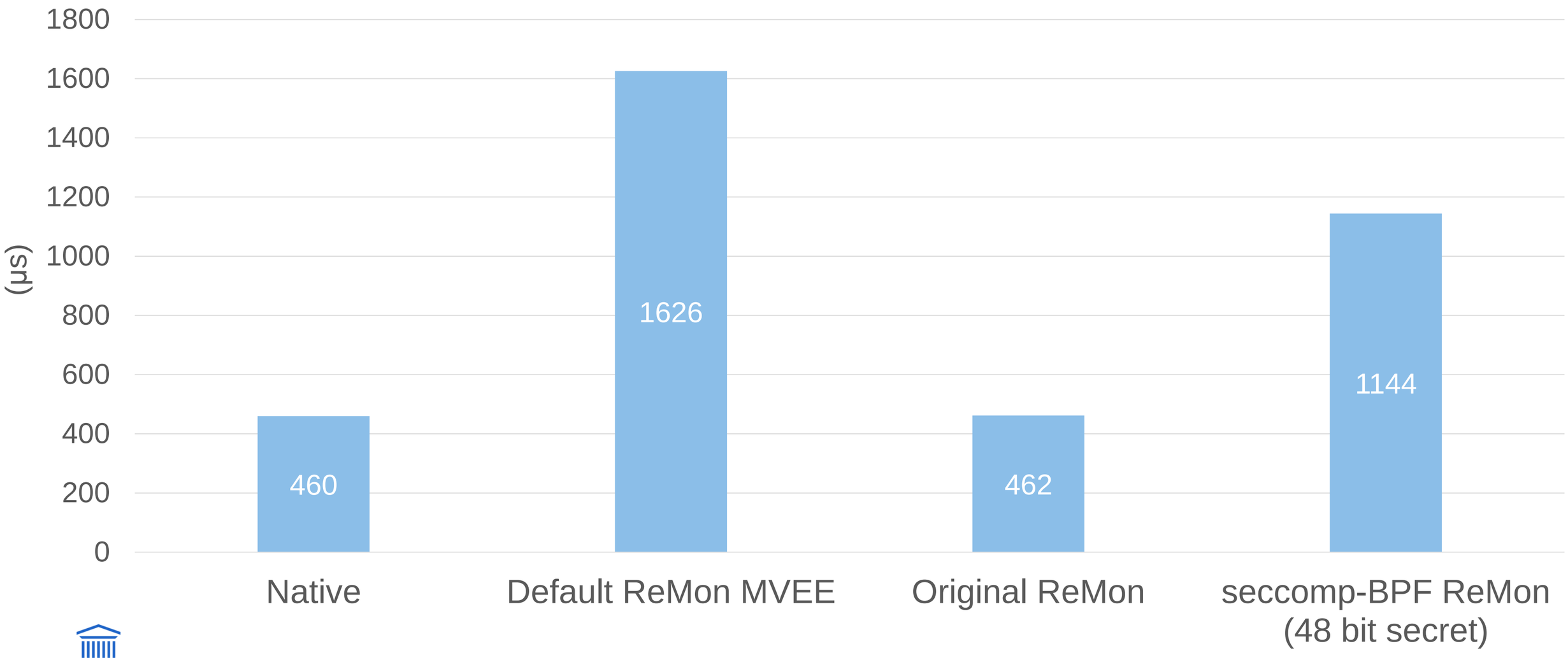
UNIVERSITEIT GENT

NGINX BENCHMARK

- Realistische applicatie
- Latency en network throughput meten
- Twee computers om realistische resultaten te verkrijgen
  - Server die nginx uitvoert onder ReMon
  - Client die aanvragen stuurt naar de server

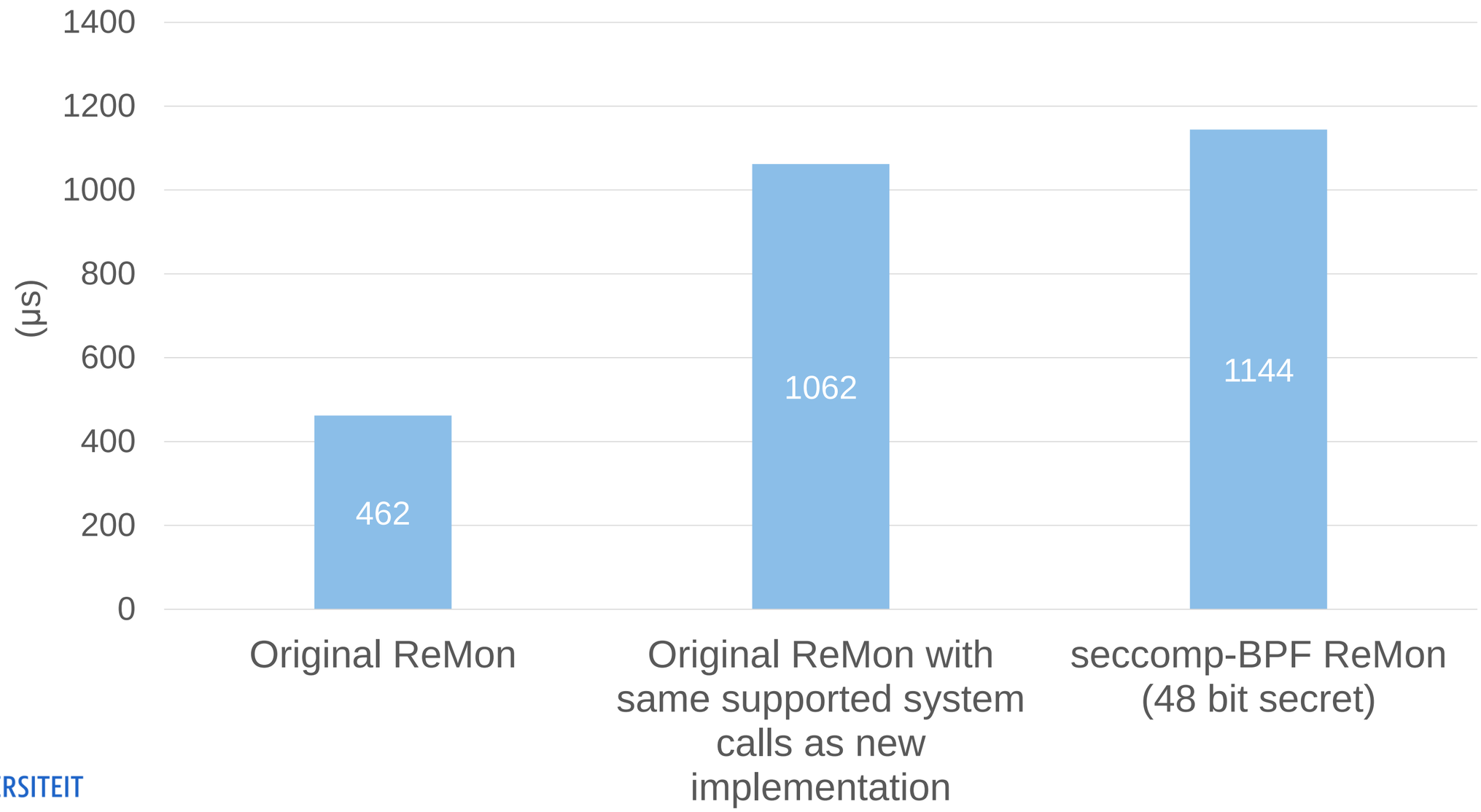
UNIVERSITEIT GENT

RESULTATEN – LATENCY



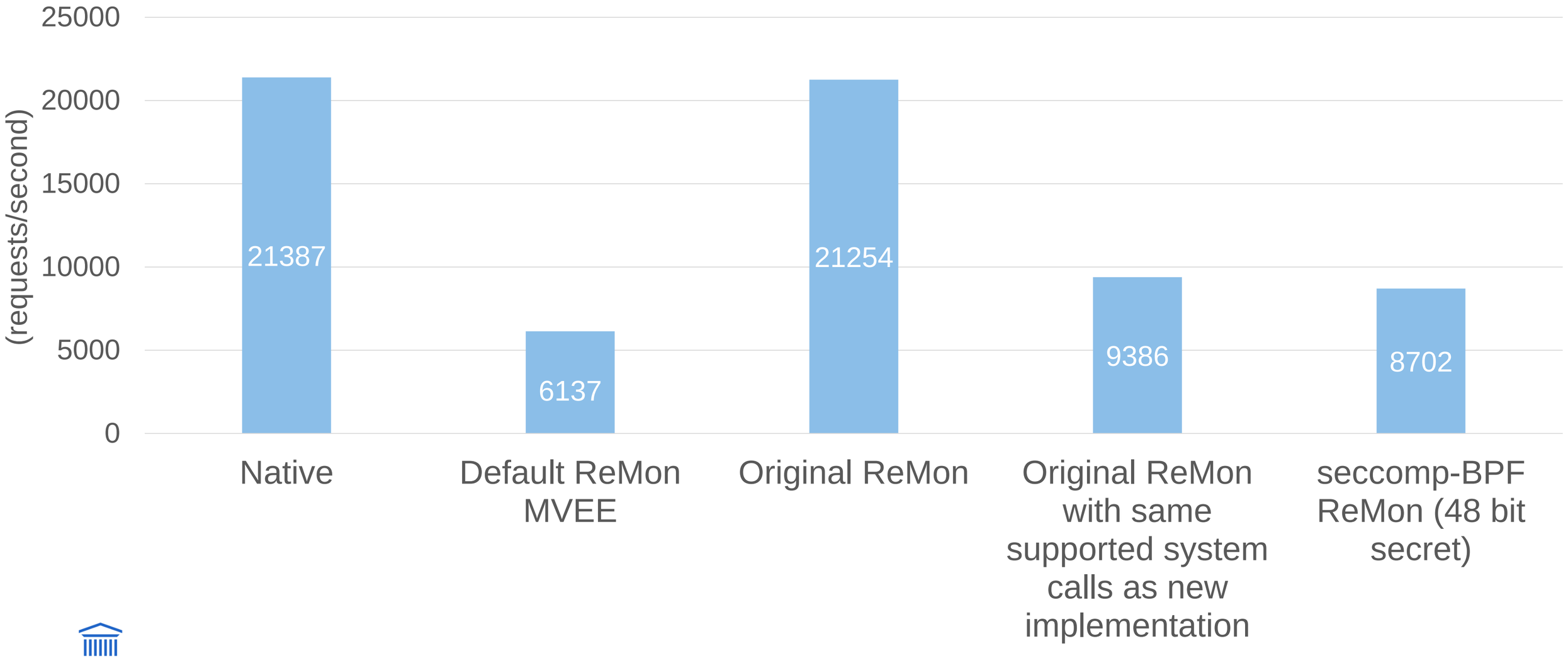
UNIVERSITEIT GENT

RESULTATEN – LATENCY GELIJKE SET



UNIVERSITEIT GENT

RESULTATEN – THROUGHPUT



UNIVERSITEIT GENT

CONCLUSIE

UNIVERSITEIT
GENT

CONCLUSIE

- Kernelpatch kan vervangen worden d.m.v. seccomp-BPF
- Snelheidswinst t.o.v. traditionele MVEE
- Snelheid in zelfde grootteorde als originele ReMon
- Verder onderzoek naar ondersteunde systeemaanroepen in nieuwe versie van IP-MON

VRAGEN

UNIVERSITEIT
GENT