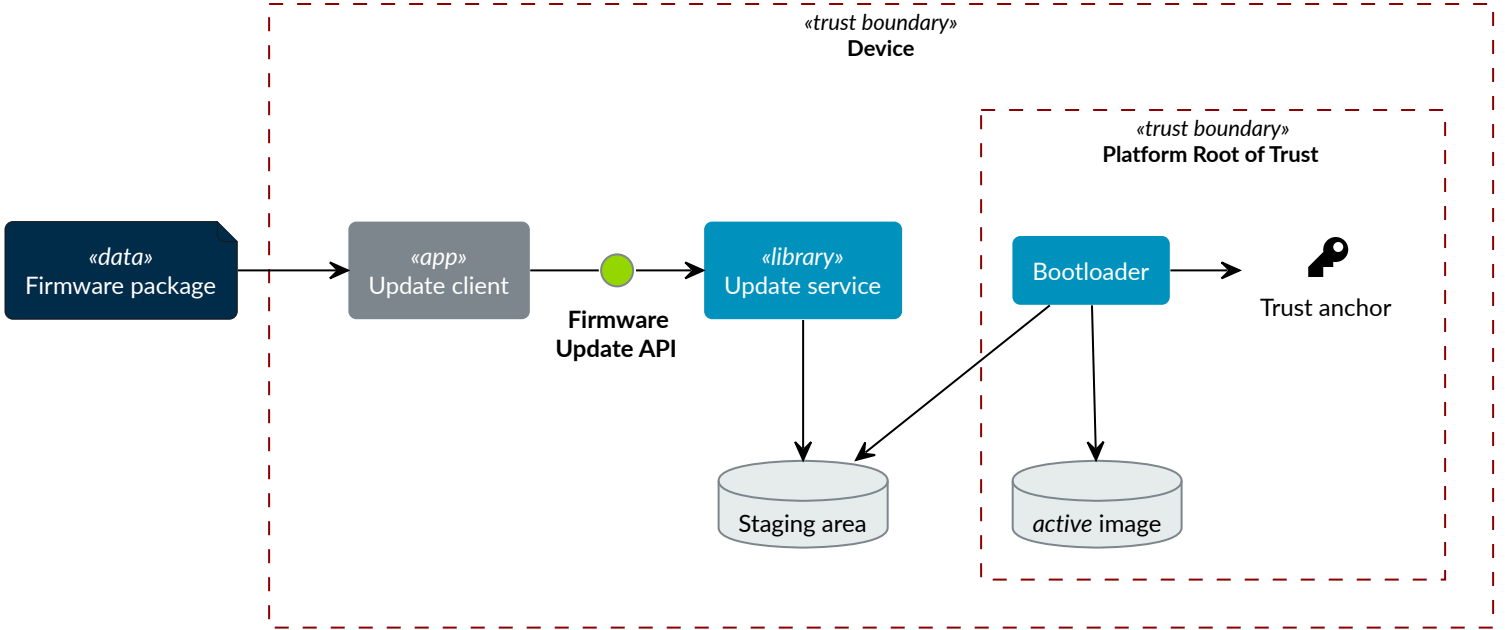
«trust boundary»
Device
«trust boundary»
Platform Root of Trust
«data»
Firmware package
«app»
Update client
Firmware
Update API
«library»
Update service
Bootloader
Trust anchor
Staging area
active image