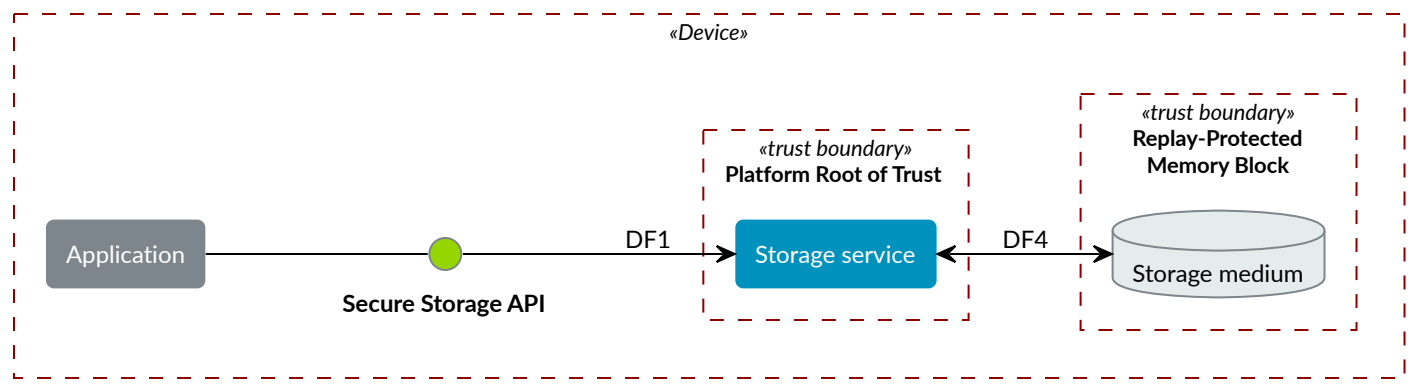
«Device»
«trust boundary»
Platform Root of Trust
«trust boundary»
Replay-Protected
Memory Block
Application
DF1
Storage service
DF4
Storage medium
Secure Storage API