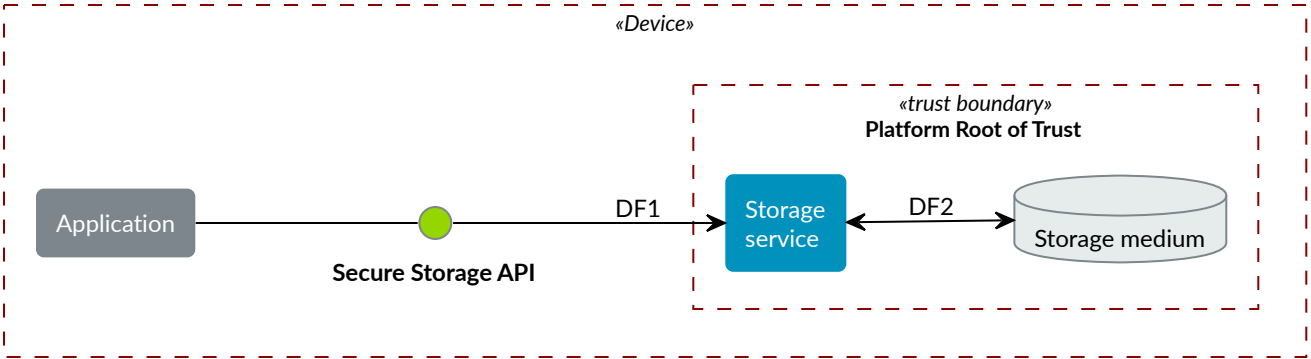
«Device»
«trust boundary»
Platform Root of Trust
Application
DF1
Storage service
DF2
Storage medium
Secure Storage API