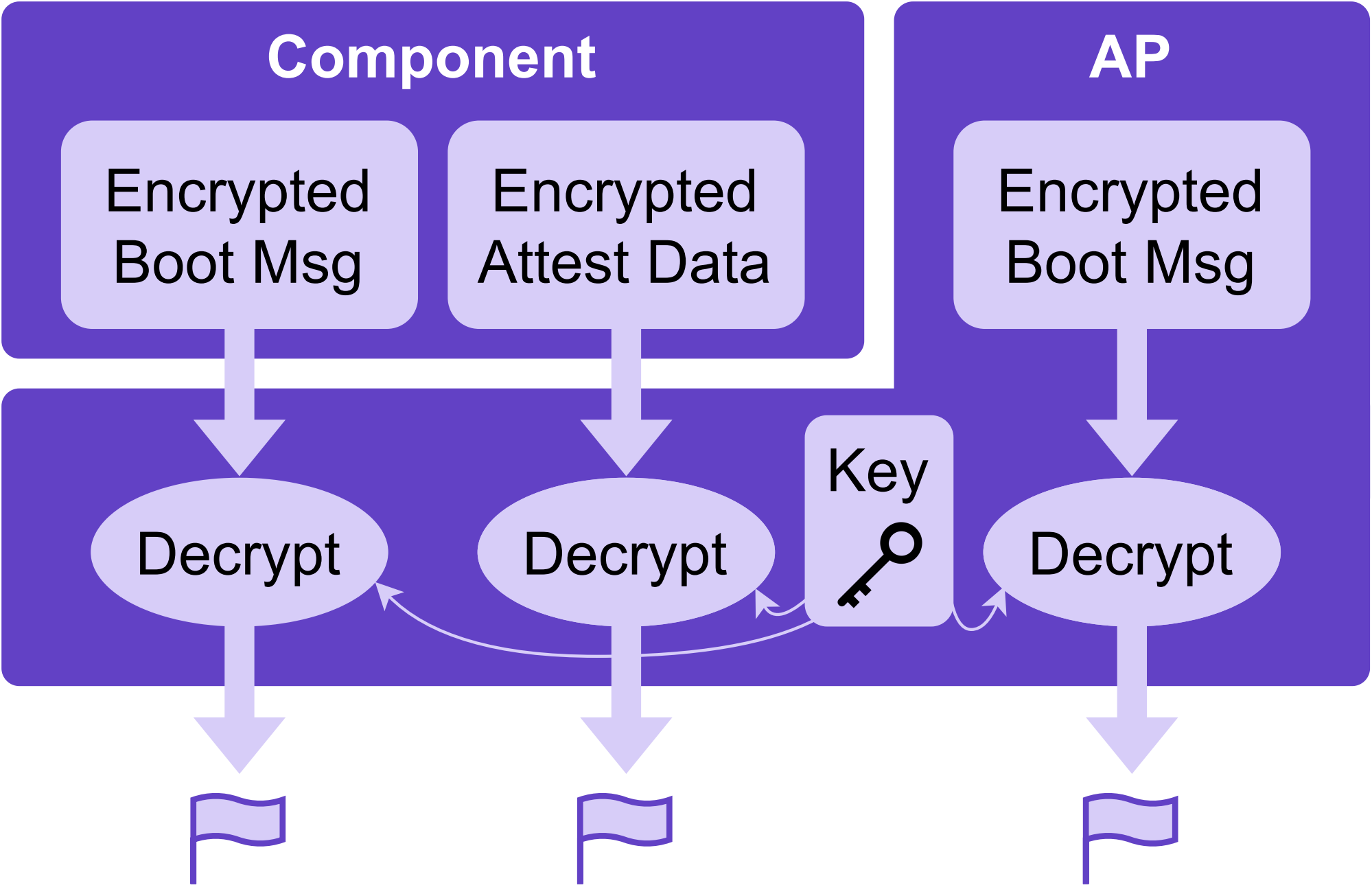
Component
AP
Encrypted Boot Msg
Encrypted Attest Data
Encrypted Boot Msg
Key
Decrypt
Decrypt
Decrypt