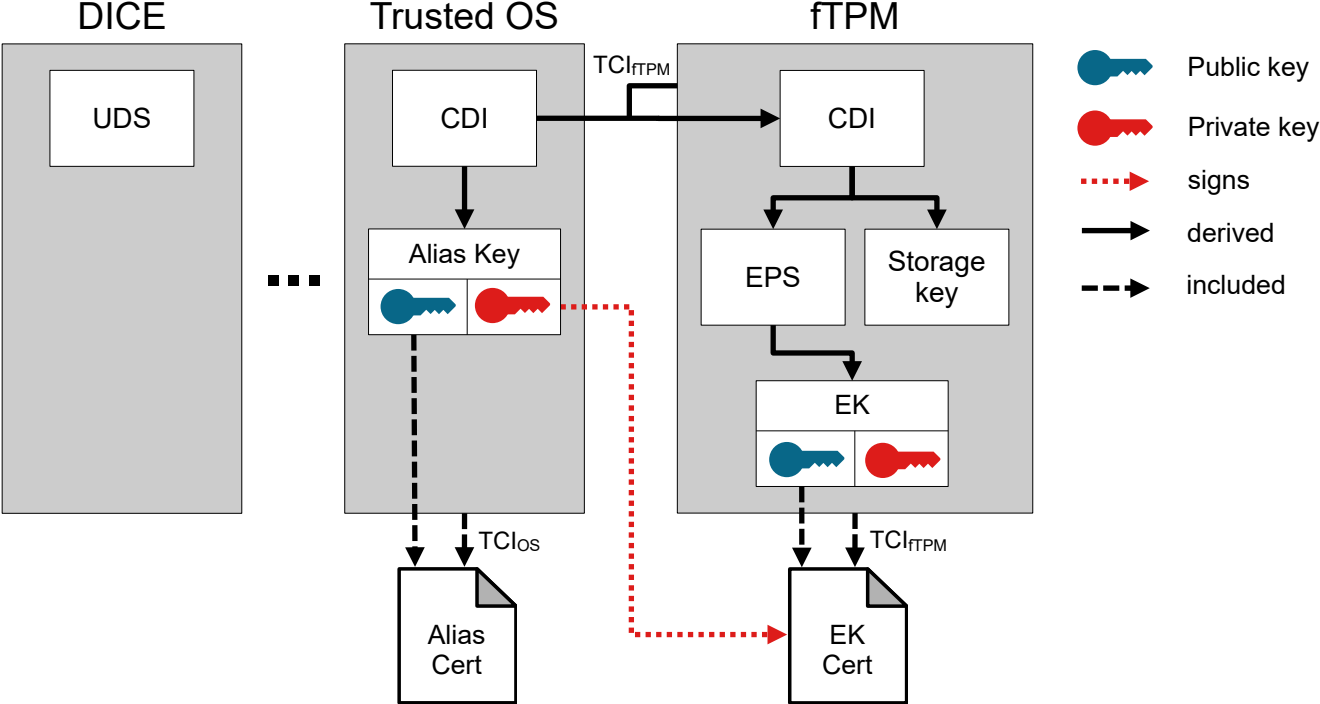
DICE
Trusted OS
fTPM
UDS
CDI
TCI$_{fTPM}$
CDI
Alias Key
EPS
Storage key
EK
TCI$_{OS}$
TCI$_{fTPM}$
Alias Cert
EK Cert
Public key
Private key
signs
derived
included