

FPGA

Application Processor

TPM

4) Perform signing
with the private
LDevID-key
and return the
resulting signature

Shared
Memory

5)
Signatur

Stack Processor

eCos
(Mbed-TLS)

5)

PN/EIP-
Stack

2)

3) Signing Request
for the Hash of all
previous TLS messages

2)

6) Certificate
Verfiy

ETH

1) Server-Hello
(Certificate Request)

MbedTLS expects
the private key to be available
locally
--> MbedTLS must be
configured/extended
so that it delegates signature requests
to the application
(instead of signing them itself).
--> Using `ifdef` + `define`,
the customer can set
this in the application processor

