1 Demo4 Diagrams

1.1 Message Sequence Diagram

$A \rightarrow B : d, N_A, PCR_{\mathrm{m}}$ on C_{AB}

$B \rightarrow T : make\_and\_load\_identity$ on C_{BT}

$T \rightarrow B : AIK^{+}, AIK_{\mathrm{h}}$ on C_{TB}

$B \rightarrow C : B, AIK^{+}$ on C_{BC}

$C \rightarrow B : \{K, \mid AIK \mid\}_{EK^{+}}, \{\{\mid AIK^{+} \mid\}_{CA^{-}}\}_{K^{+}}$ on C_{CB}

$B \rightarrow T : activate\_identity(AIK_{\mathrm{h}}, \mid AIK \mid)$ on C_{BT}

$T \rightarrow B : K$ on C_{TB}

$B \rightarrow M : d$ on C_{BM}

$M \rightarrow B : e$ on C_{MB}

$B \rightarrow T : quote(\ AIK_{\mathrm{h}}, PCR_{\mathrm{m}}, \mid (e, N_A, \{\mid AIK^{+} \mid\}_{CA^{-}}) \mid)$ on C_{BT}

$T \rightarrow B : PCR_{\mathrm{c}}, \{\mid\mid PCR_{\mathrm{c}} \mid, \mid (e, N_A, \{\mid AIK^{+} \mid\}_{CA^{-}}) \mid\mid\}_{AIK^{-}}$ on C_{TB}

$B \rightarrow A : e, N_A, PCR_{\mathrm{c}}, \{\mid AIK^{+} \mid\}_{CA^{-}}$ on C_{BA}

$B \rightarrow A : \{\mid\mid PCR_{\mathrm{c}} \mid, \mid (e, N_A, \{\mid AIK^{+} \mid\}_{CA^{-}}) \mid\mid\}_{AIK^{-}}$ on C_{BA}

KEY

A:	Appraiser
B:	Attestation Agent
T:	TPM
C:	Certificate Authority
M:	Measurer
d :	desired evidence
e :	gathered evidence
N_A :	nonce generated by A
$\mathrm{PCR_m}$:	pcr mask indicating desired pcr registers
$\mathrm{PCR_c}$:	pcr composite structure containing select pcr register values
$\mathrm{AIK_h}$:	AIK key handle(used by TPM to reference loaded keys)
K:	Session key created by C

1.2 Strand Space Diagram