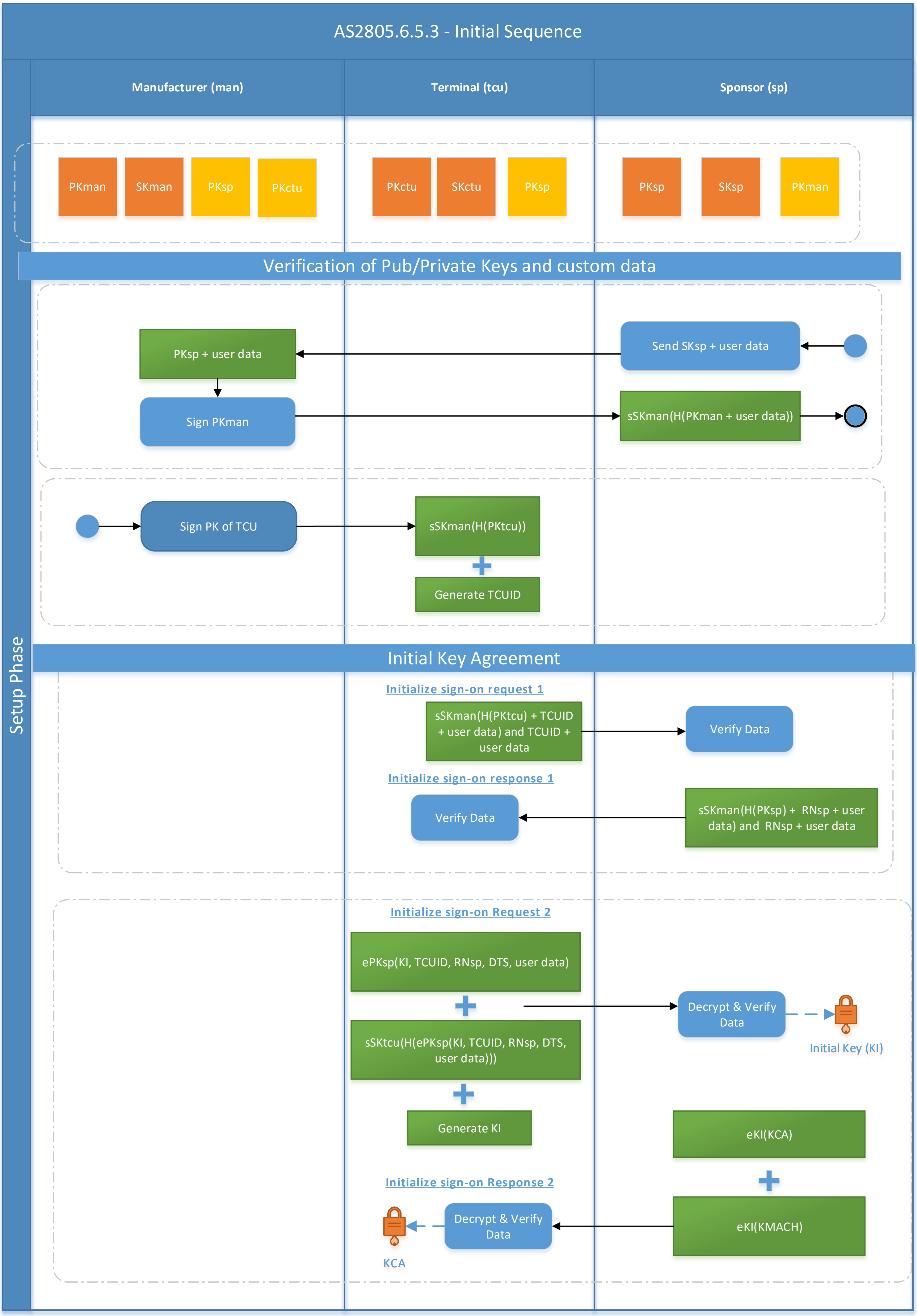
AS2805.6.5.3 - Initial Sequence



Setup Phase

Manufacturer (man)

Terminal (tcu)

Sponsor (sp)

PKman

SKman

PKsp

PKctu

PKctu

SKctu

PKsp

PKsp

SKsp

PKman

Verification of Pub/Private Keys and custom data

Send SKsp + user data

PKsp + user data

Sign PKman

sSKman(H(PKman + user data))

Sign PK of TCU

sSKman(H(PKtcu))

Generate TCUID

Initial Key Agreement

Initialize sign-on request 1

sSKman(H(PKtcu) + TCUID + user data) and TCUID + user data

Verify Data

Initialize sign-on response 1

sSKman(H(PKsp) + RNsp + user data) and RNsp + user data

Verify Data

Initialize sign-on Request 2

ePKsp(KI, TCUID, RNsp, DTS, user data)

sSKtcu(H(ePKsp(KI, TCUID, RNsp, DTS, user data)))

Generate KI

Decrypt & Verify Data

Initial Key (KI)

eKI(KCA)

eKI(KMACH)

Initialize sign-on Response 2

Decrypt & Verify Data

KCA