

# AS2805.6.5.3 - Initial Sequence

Manufacturer (man)

Terminal (tcu)

Sponsor (sp)

PKman

SKman

PKsp

PKctu

PKctu

SKctu

PKsp

PKsp

SKsp

PKman

## Verification of Pub/Private Keys and custom data

PKsp, user data

Send PKsp, user data

Sign PKman

sSKman(H(PKman | user data))

Sign PK of TCU

sSKman(H(PKctu))

Generate TCUID

## Initial Key Agreement

### Initialize sign-on request 1

sSKman(H(PKctu) | TCUID | user data) and TCUID, user data

Verify Data

### Initialize sign-on response 1

Verify Data

sSKman(H(PKsp) | RNsp | user data) and RNsp, user 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)

### Initialize sign-on Response 2

KCA

Decrypt & Verify Data

eKI(KMACH)

Setup Phase