secure channel testing

purpose

- confirm osdp_CHLNG, osdp_CCRYPT, osdp_SCRYPT, osdp_RMAC_I are working
- confirm SCS headers 11-18 are working
- test both default and paired base key and KEYSET
- test key management and perform minimal lockdown checks

process group 1 check secure channel

1. prepare PD. reset to initial unpaired state. use factory reset and then osdp secure channel control card to set reader into reset state.
2. start ACU (in the clear)
3. establish secure channel session using default key
4. confirm session is stable for at least 8 poll-ack cycles after the RMAC_I
5. check SCS headers in session negotiation
6. osdp_CAP to induce PD to send encrypted response payload
7. osdp_LED to send encrypted command payload

process group 2 pairing

1. given PD in secure channel on base key, issue osdp_KEYSET
2. confirm link remains stable on existing session
3. stop ACU
4. start ACU (in the clear). confirm PD behaves rationally.
5. initiate secure channel session on paired key
6. confirm link is stable on paired key session
7. perform card read or keypress confirm data arrives intact

process group 3 key rotation

1. set up PD with a paired key
2. within that secure channel session issue a KEYSET for a new key
3. confirm proper behavior after keyset
4. stop/start ACU and confirm paired key operation on the new key

process group 4 lockdown check

1. set up with a paired key
2. confirm it doesn't work in the clear any more
3. confirm a default key session can't be established
4. given reset and unpaired reader confirm rational response to rogue paired challenge