Bluetooth Baseband LSI

Panasonic PAN1026

Toshiba TC35661

SMP

Message Sequence Chart

October.2013

000630EBA1-000809TS

- PANASONIC is continually working to improve the quality and reliability of its products. Nevertheless, semiconductor devices in general can malfunction or fail due to their inherent electrical sensitivity and vulnerability to physical stress. It is the responsibility of the buyer, when utilizing PANASONIC products, to comply with the standards of safety in making a safe design for the entire system, and to avoid situations in which a malfunction or failure of such PANASONIC products could cause loss of human life, bodily injury or damage to property.
  In developing your designs, please ensure that PANASONIC products are used within specified operating ranges as set forth in the most recent PANASONIC products specifications.
- The PANASONIC products listed in this document are intended for usage in general electronics applications (computer, personal equipment, office equipment, measuring equipment, industrial robotics, domestic appliances, etc.). These PANASONIC products are neither intended nor warranted for usage in equipment that requires extraordinarily high quality and/or reliability or a malfunction or failure of which may cause loss of human life or bodily injury ("Unintended Usage"). Unintended Usage include atomic energy control instruments, airplane or spaceship instruments, transportation instruments, traffic signal instruments, combustion control instruments, medical instruments, all types of safety devices, etc.. Unintended Usage of PANASONIC products listed in this document shall be made at the customer's own risk.
- The products described in this document are subject to the foreign exchange and foreign trade laws.
- The information contained herein is presented only as a guide for the applications of our products. No responsibility is assumed by PANASONIC CORPORATION for any infringements of intellectual property or other rights of the third parties which may result from its use. No license is granted by implication or otherwise under any intellectual property or other rights of PANASONIC CORPORATION or others.
- The information contained herein is subject to change without notice.
- The information contained herein is presented only as a guide for the product operation, its functions, and applications. We request that the operation of any application system incorporating this product is fully tested by system vendor.

Revision History

Date	Modification	Note
19th-August-2013	1st Release	
3rd-October-2013	Added the explanations to the following chapters: 1.1 Initial Setting -> Connection -> ... 1.2 Connection -> Authentication(JustWork,LTK) from Central .... 1.4 Key update Added the following chapter: 1.3 Connection -> Authentication(JustWork,LTK) from Peripheral -> Disconnection	

CONTENT

1. MSC ····· 5

1.1 Initial Setting -> Connection -> Authentication(JustWork,LTK) from Central -> Disconnection ····· 5

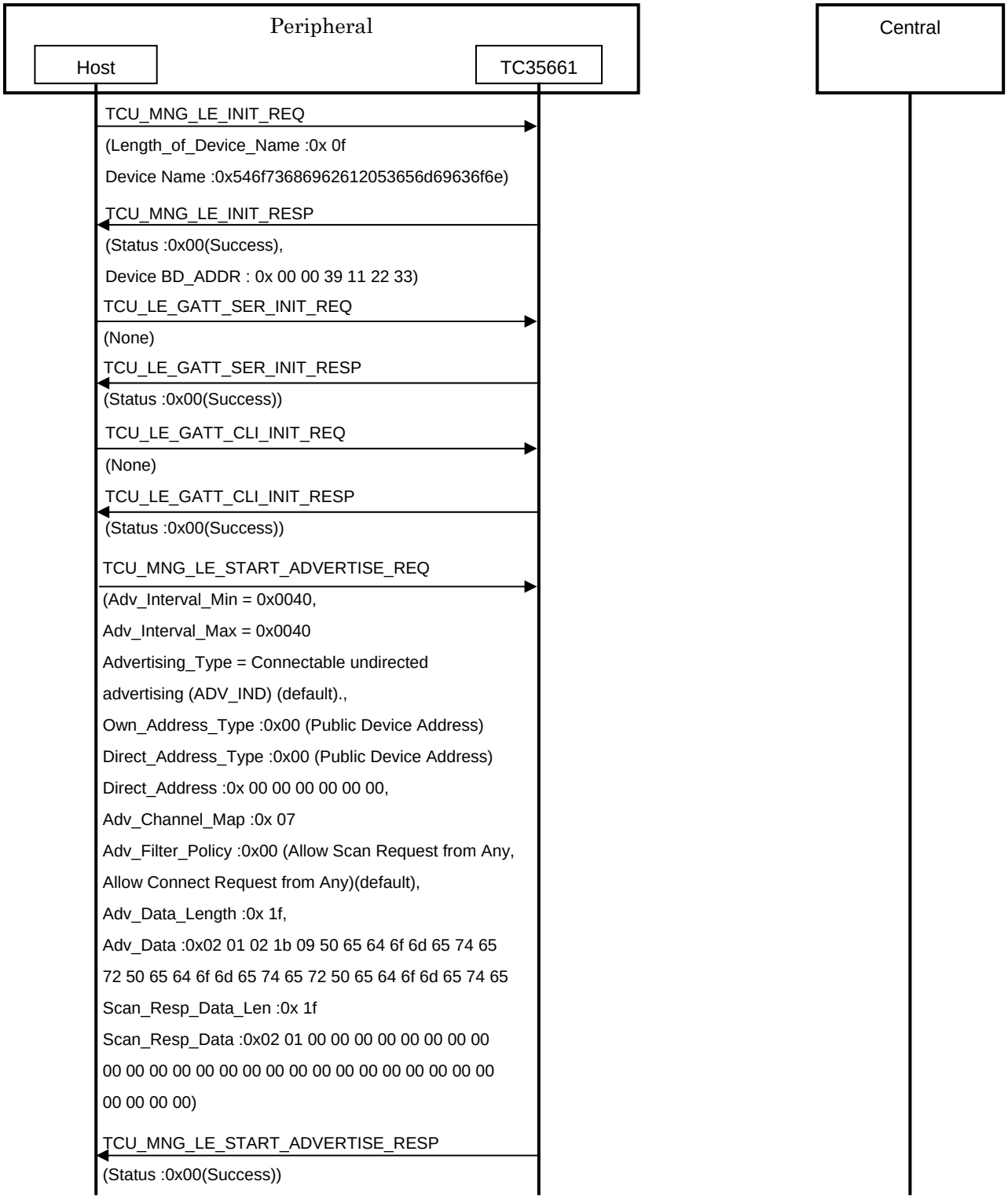
1.2 Connection -> Authentication(JustWork,LTK) from Central -> Disconnection -> Reconnection -> Encryption -> Disconnection ····· 9

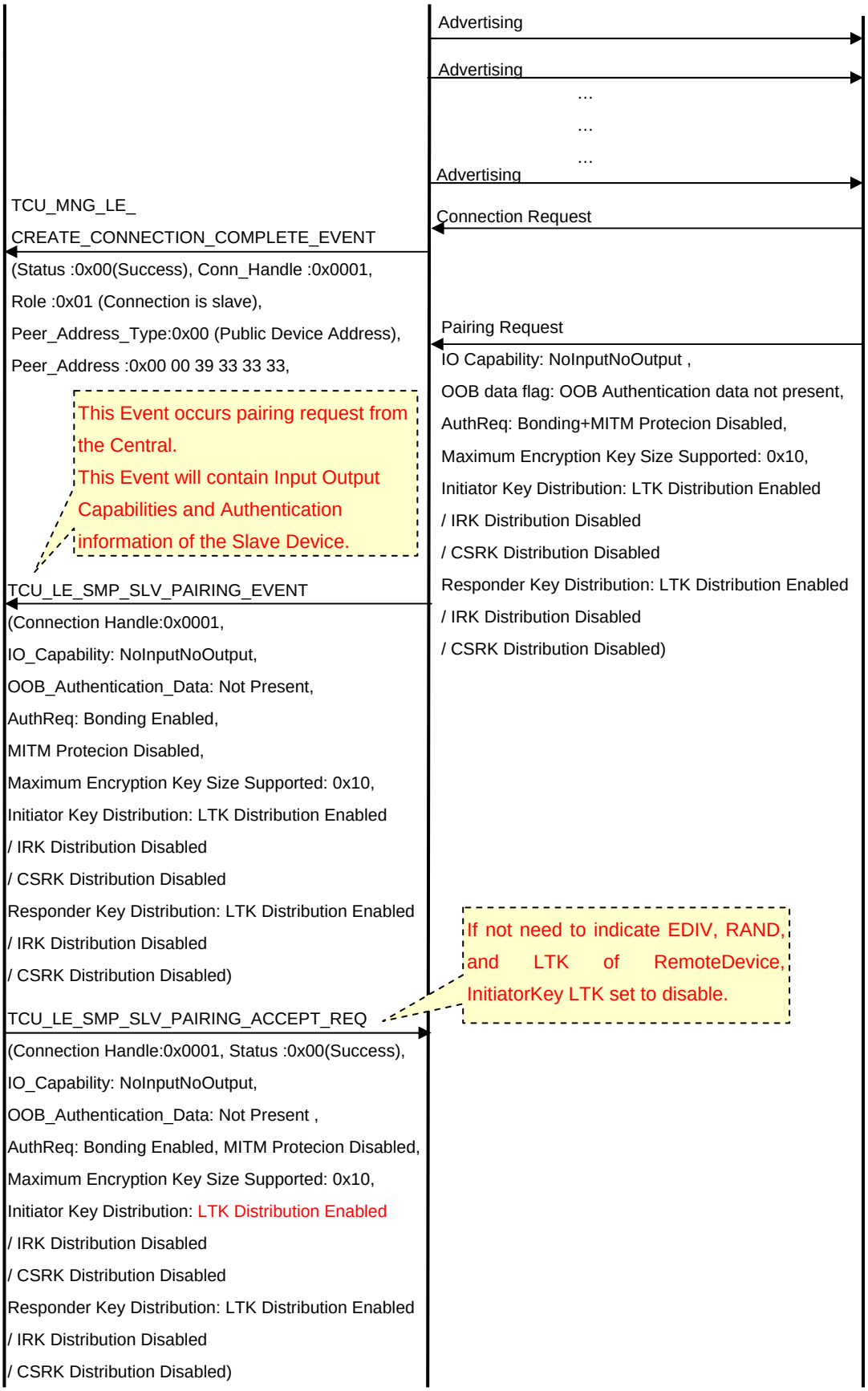
1.3 Connection -> Authentication(JustWork,LTK) from Peripheral -> Disconnection14

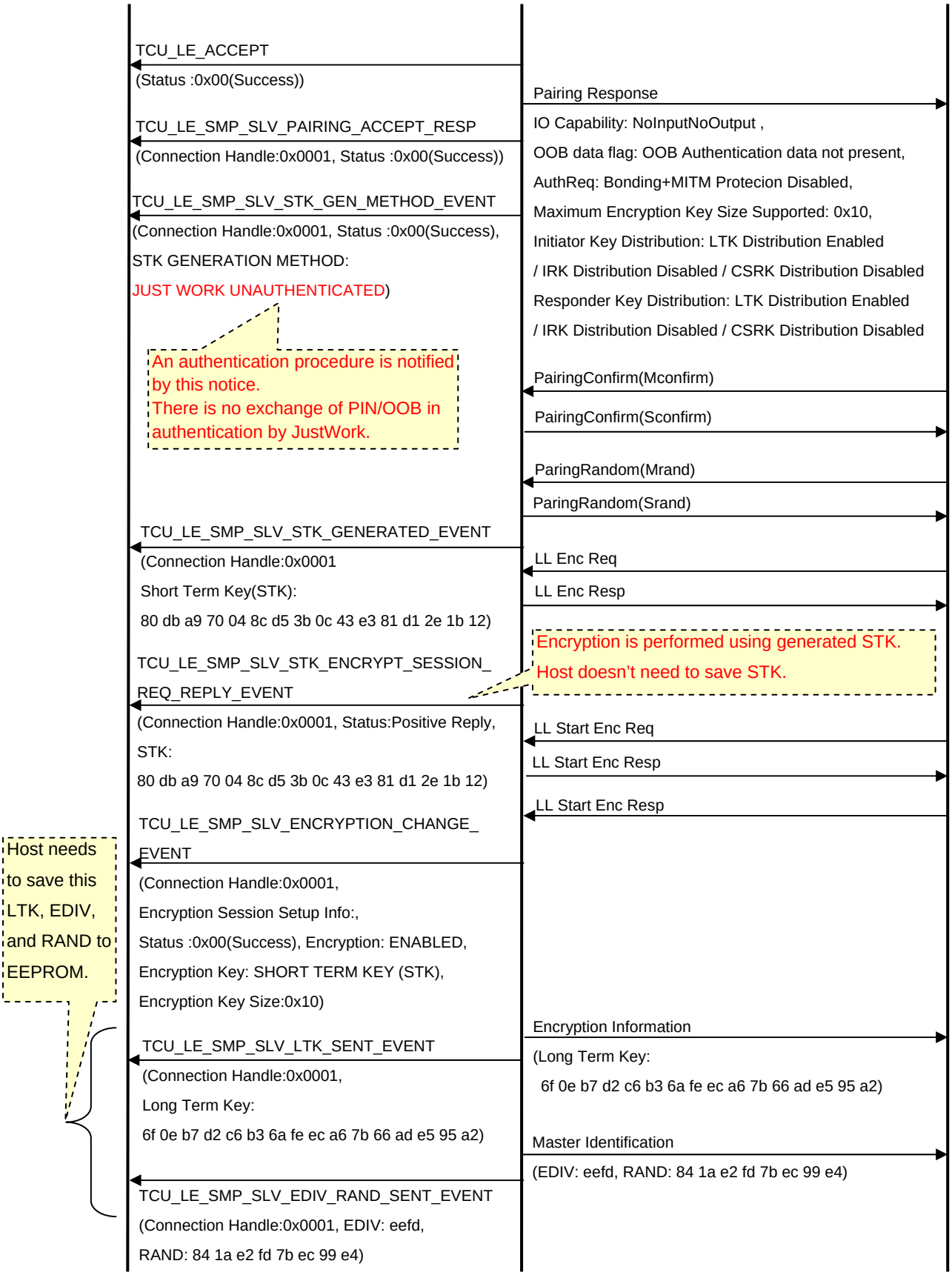
1.4 Key update····· 18

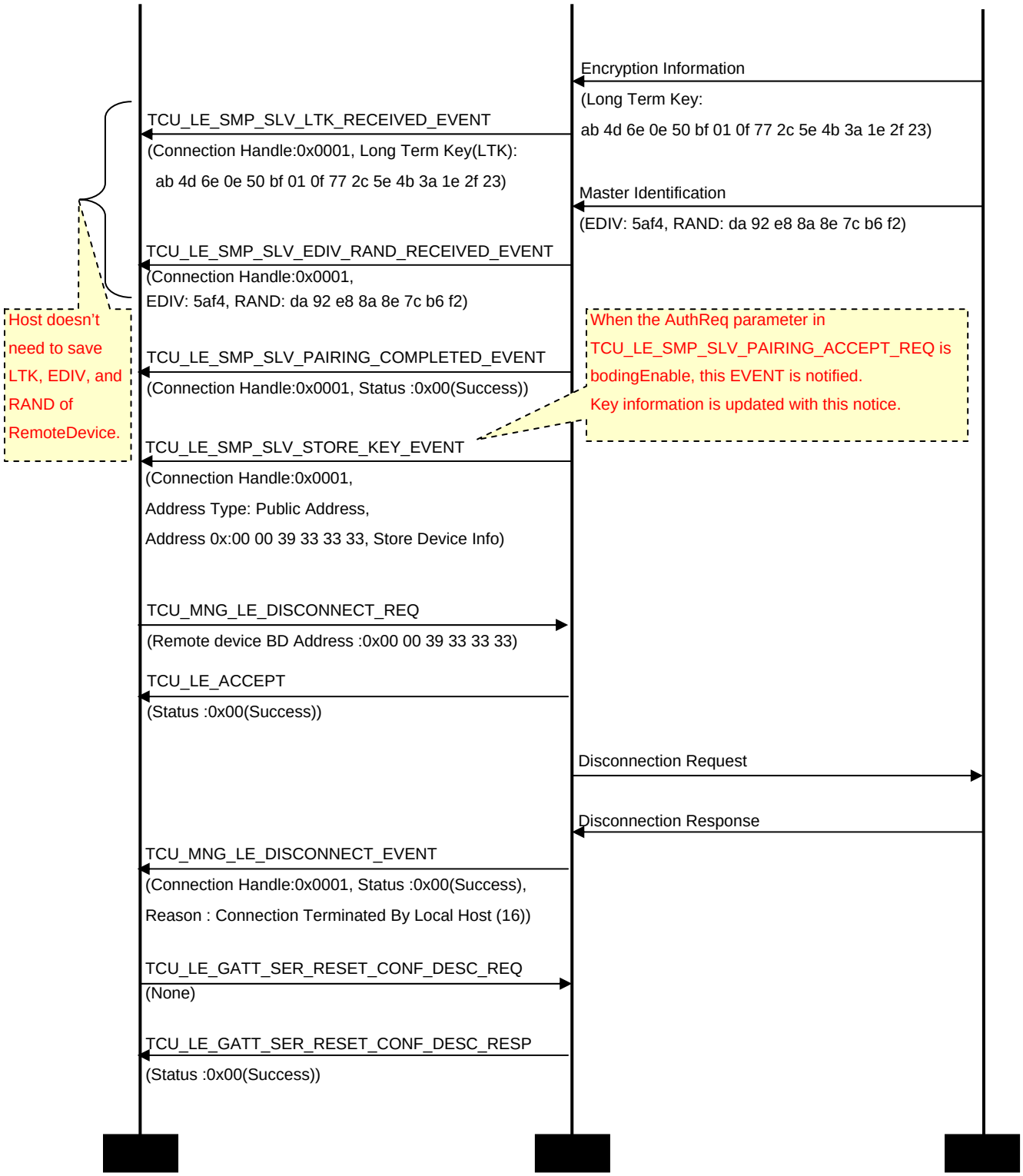
1. MSC

1.1 Initial Setting -> Connection -> Authentication(JustWork,LTK) from Central -> Disconnection

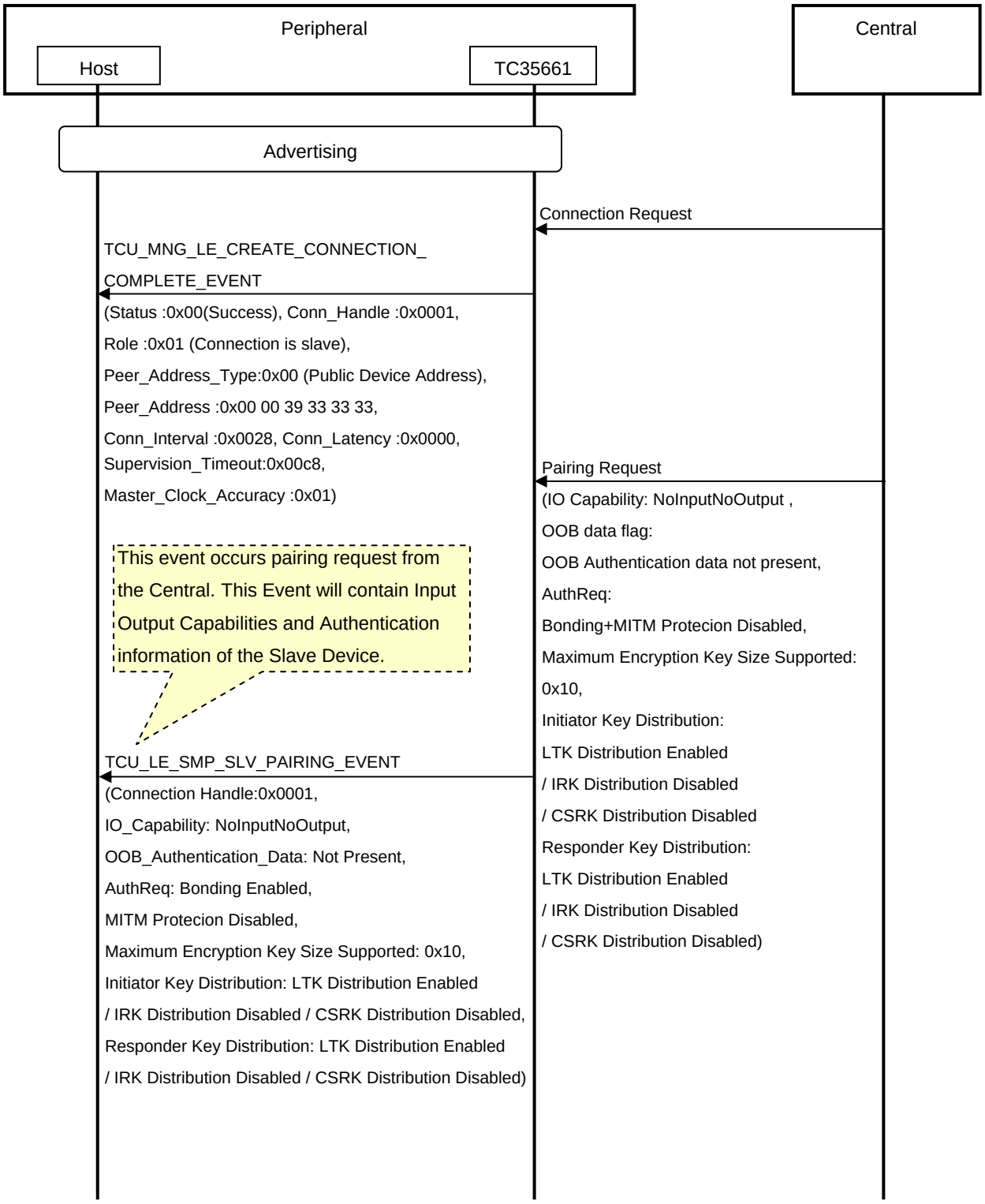


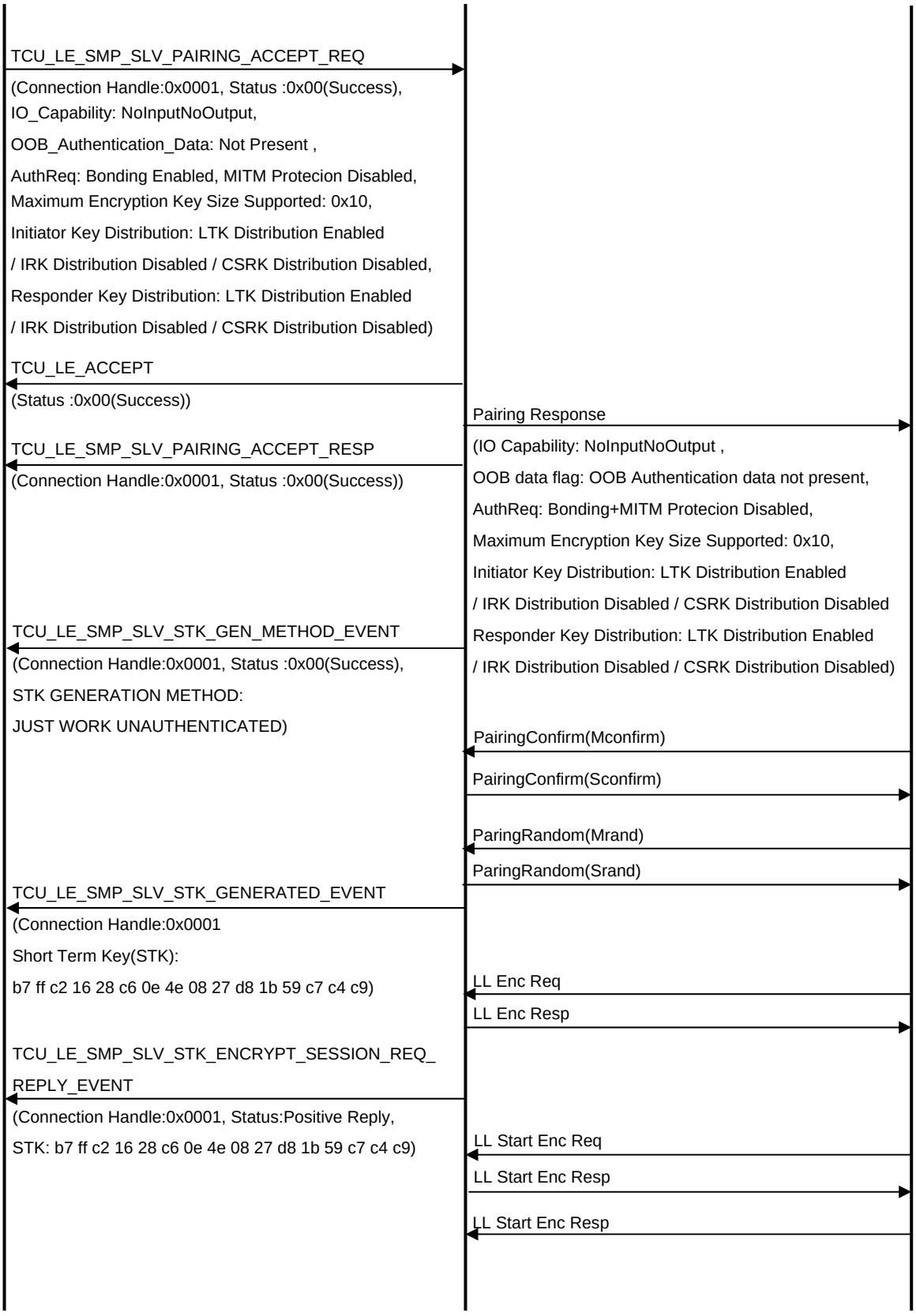

Advertising
Advertising
...
...
...
Advertising
TCU_MNG_LE_
CREATE_CONNECTION_COMPLETE_EVENT
(Status :0x00(Success), Conn_Handle :0x0001,
Role :0x01 (Connection is slave),
Peer_Address_Type:0x00 (Public Device Address),
Peer_Address :0x00 00 39 33 33 33,
Connection Request
Pairing Request
IO Capability: NoInputNoOutput ,
OOB data flag: OOB Authentication data not present,
AuthReq: Bonding+MITM Protecion Disabled,
Maximum Encryption Key Size Supported: 0x10,
Initiator Key Distribution: LTK Distribution Enabled
/ IRK Distribution Disabled
/ CSRK Distribution Disabled
Responder Key Distribution: LTK Distribution Enabled
/ IRK Distribution Disabled
/ CSRK Distribution Disabled)
This Event occurs pairing request from the Central.
This Event will contain Input Output Capabilities and Authentication information of the Slave Device.
TCU_LE_SMP_SLV_PAIRING_EVENT
(Connection Handle:0x0001,
IO_Capability: NoInputNoOutput,
OOB_Authentication_Data: Not Present,
AuthReq: Bonding Enabled,
MITM Protecion Disabled,
Maximum Encryption Key Size Supported: 0x10,
Initiator Key Distribution: LTK Distribution Enabled
/ IRK Distribution Disabled
/ CSRK Distribution Disabled
Responder Key Distribution: LTK Distribution Enabled
/ IRK Distribution Disabled
/ CSRK Distribution Disabled)
If not need to indicate EDIV, RAND, and LTK of RemoteDevice, InitiatorKey LTK set to disable.
TCU_LE_SMP_SLV_PAIRING_ACCEPT_REQ
(Connection Handle:0x0001, Status :0x00(Success),
IO_Capability: NoInputNoOutput,
OOB_Authentication_Data: Not Present ,
AuthReq: Bonding Enabled, MITM Protecion Disabled,
Maximum Encryption Key Size Supported: 0x10,
Initiator Key Distribution: LTK Distribution Enabled
/ IRK Distribution Disabled
/ CSRK Distribution Disabled
Responder Key Distribution: LTK Distribution Enabled
/ IRK Distribution Disabled
/ CSRK Distribution Disabled)

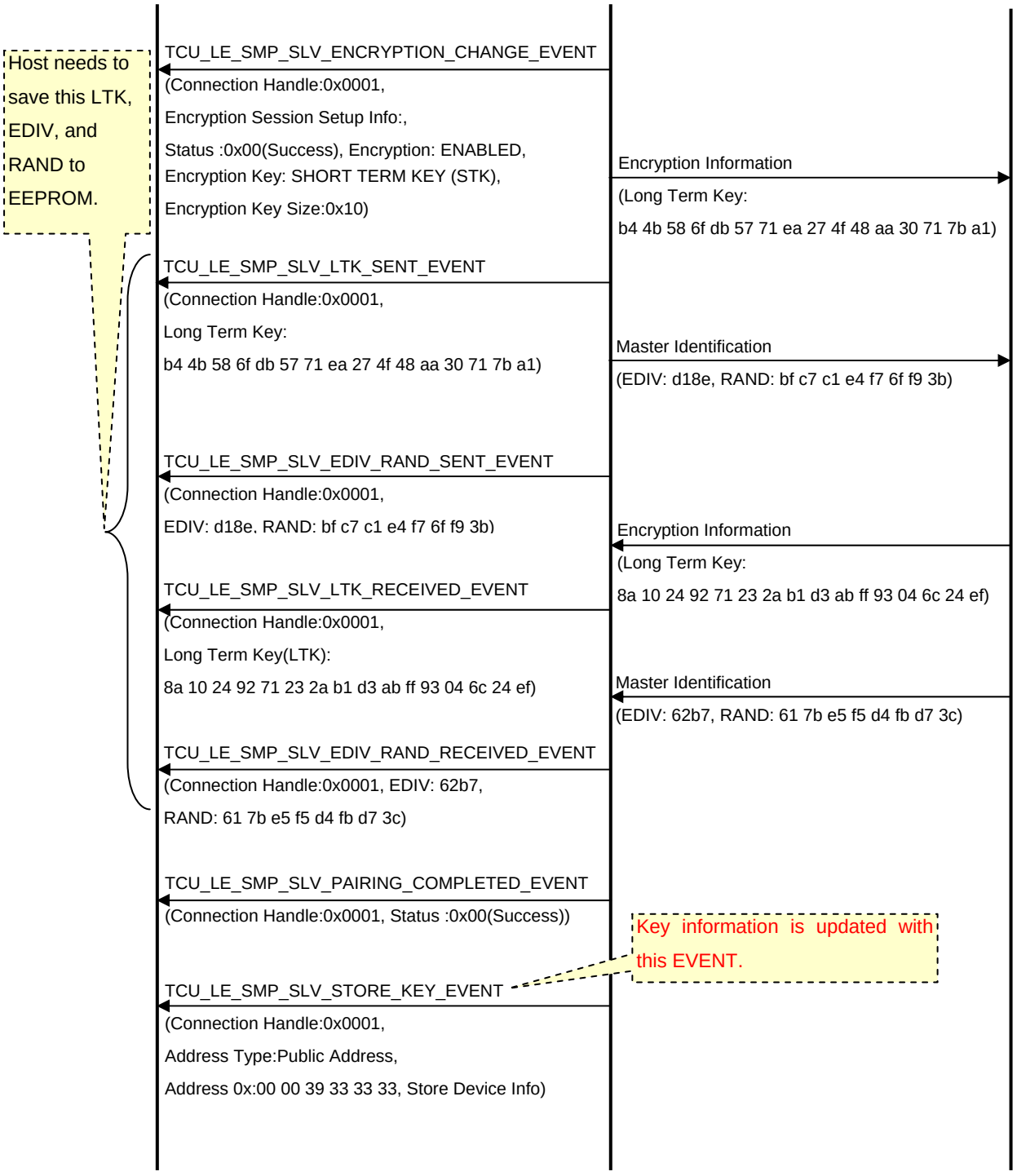

TCU_LE_ACCEPT
(Status :0x00(Success))
Pairing Response
IO Capability: NoInputNoOutput ,
OOB data flag: OOB Authentication data not present,
AuthReq: Bonding+MITM Protecion Disabled,
Maximum Encryption Key Size Supported: 0x10,
Initiator Key Distribution: LTK Distribution Enabled
/ IRK Distribution Disabled / CSRK Distribution Disabled
Responder Key Distribution: LTK Distribution Enabled
/ IRK Distribution Disabled / CSRK Distribution Disabled
TCU_LE_SMP_SLV_PAIRING_ACCEPT_RESP
(Connection Handle:0x0001, Status :0x00(Success))
TCU_LE_SMP_SLV_STK_GEN_METHOD_EVENT
(Connection Handle:0x0001, Status :0x00(Success),
STK GENERATION METHOD:
JUST WORK UNAUTHENTICATED)
An authentication procedure is notified by this notice.
There is no exchange of PIN/OOB in authentication by JustWork.
PairingConfirm(Mconfirm)
PairingConfirm(Sconfirm)
ParingRandom(Mrand)
ParingRandom(Srand)
TCU_LE_SMP_SLV_STK_GENERATED_EVENT
(Connection Handle:0x0001
Short Term Key(STK):
80 db a9 70 04 8c d5 3b 0c 43 e3 81 d1 2e 1b 12)
LL Enc Req
LL Enc Resp
Encryption is performed using generated STK.
Host doesn't need to save STK.
TCU_LE_SMP_SLV_STK_ENCRYPT_SESSION_
REQ_REPLY_EVENT
(Connection Handle:0x0001, Status:Positive Reply,
STK:
80 db a9 70 04 8c d5 3b 0c 43 e3 81 d1 2e 1b 12)
LL Start Enc Req
LL Start Enc Resp
LL Start Enc Resp
TCU_LE_SMP_SLV_ENCRYPTION_CHANGE_
EVENT
(Connection Handle:0x0001,
Encryption Session Setup Info:,
Status :0x00(Success), Encryption: ENABLED,
Encryption Key: SHORT TERM KEY (STK),
Encryption Key Size:0x10)
Host needs to save this LTK, EDIV, and RAND to EEPROM.
Encryption Information
(Long Term Key:
6f 0e b7 d2 c6 b3 6a fe ec a6 7b 66 ad e5 95 a2)
TCU_LE_SMP_SLV_LTK_SENT_EVENT
(Connection Handle:0x0001,
Long Term Key:
6f 0e b7 d2 c6 b3 6a fe ec a6 7b 66 ad e5 95 a2)
Master Identification
(EDIV: eefd, RAND: 84 1a e2 fd 7b ec 99 e4)
TCU_LE_SMP_SLV_EDIV_RAND_SENT_EVENT
(Connection Handle:0x0001, EDIV: eefd,
RAND: 84 1a e2 fd 7b ec 99 e4)

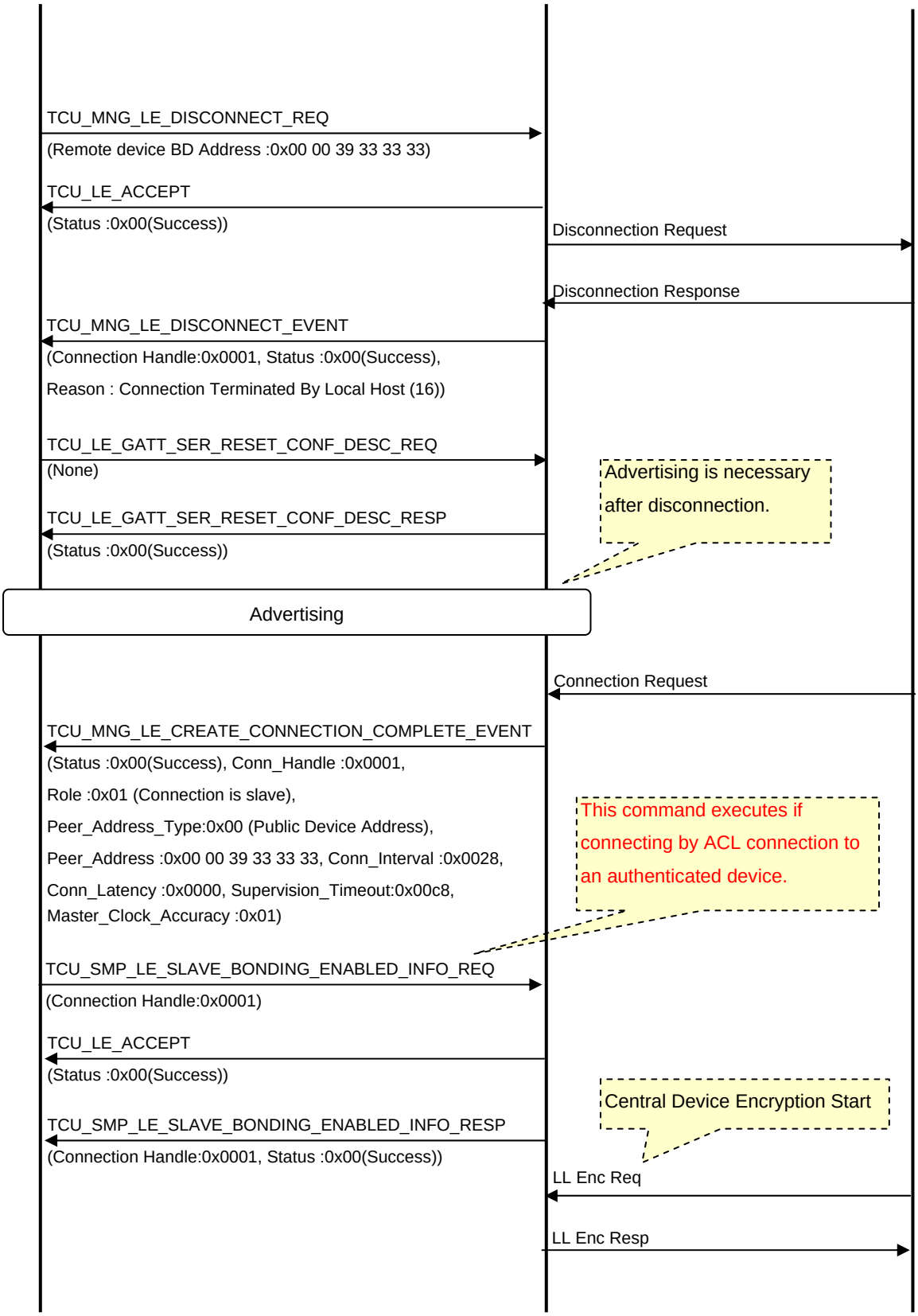

Encryption Information
(Long Term Key:
ab 4d 6e 0e 50 bf 01 0f 77 2c 5e 4b 3a 1e 2f 23)
TCU_LE_SMP_SLV_LTK_RECEIVED_EVENT
(Connection Handle:0x0001, Long Term Key(LTK):
ab 4d 6e 0e 50 bf 01 0f 77 2c 5e 4b 3a 1e 2f 23)
Master Identification
(EDIV: 5af4, RAND: da 92 e8 8a 8e 7c b6 f2)
TCU_LE_SMP_SLV_EDIV_RAND_RECEIVED_EVENT
(Connection Handle:0x0001,
EDIV: 5af4, RAND: da 92 e8 8a 8e 7c b6 f2)
Host doesn't need to save LTK, EDIV, and RAND of RemoteDevice.
When the AuthReq parameter in TCU_LE_SMP_SLV_PAIRING_ACCEPT_REQ is bodingEnable, this EVENT is notified.
Key information is updated with this notice.
TCU_LE_SMP_SLV_PAIRING_COMPLETED_EVENT
(Connection Handle:0x0001, Status :0x00(Success))
TCU_LE_SMP_SLV_STORE_KEY_EVENT
(Connection Handle:0x0001,
Address Type: Public Address,
Address 0x:00 00 39 33 33 33, Store Device Info)
TCU_MNG_LE_DISCONNECT_REQ
(Remote device BD Address :0x00 00 39 33 33 33)
TCU_LE_ACCEPT
(Status :0x00(Success))
Disconnection Request
Disconnection Response
TCU_MNG_LE_DISCONNECT_EVENT
(Connection Handle:0x0001, Status :0x00(Success),
Reason : Connection Terminated By Local Host (16))
TCU_LE_GATT_SER_RESET_CONF_DESC_REQ
(None)
TCU_LE_GATT_SER_RESET_CONF_DESC_RESP
(Status :0x00(Success))

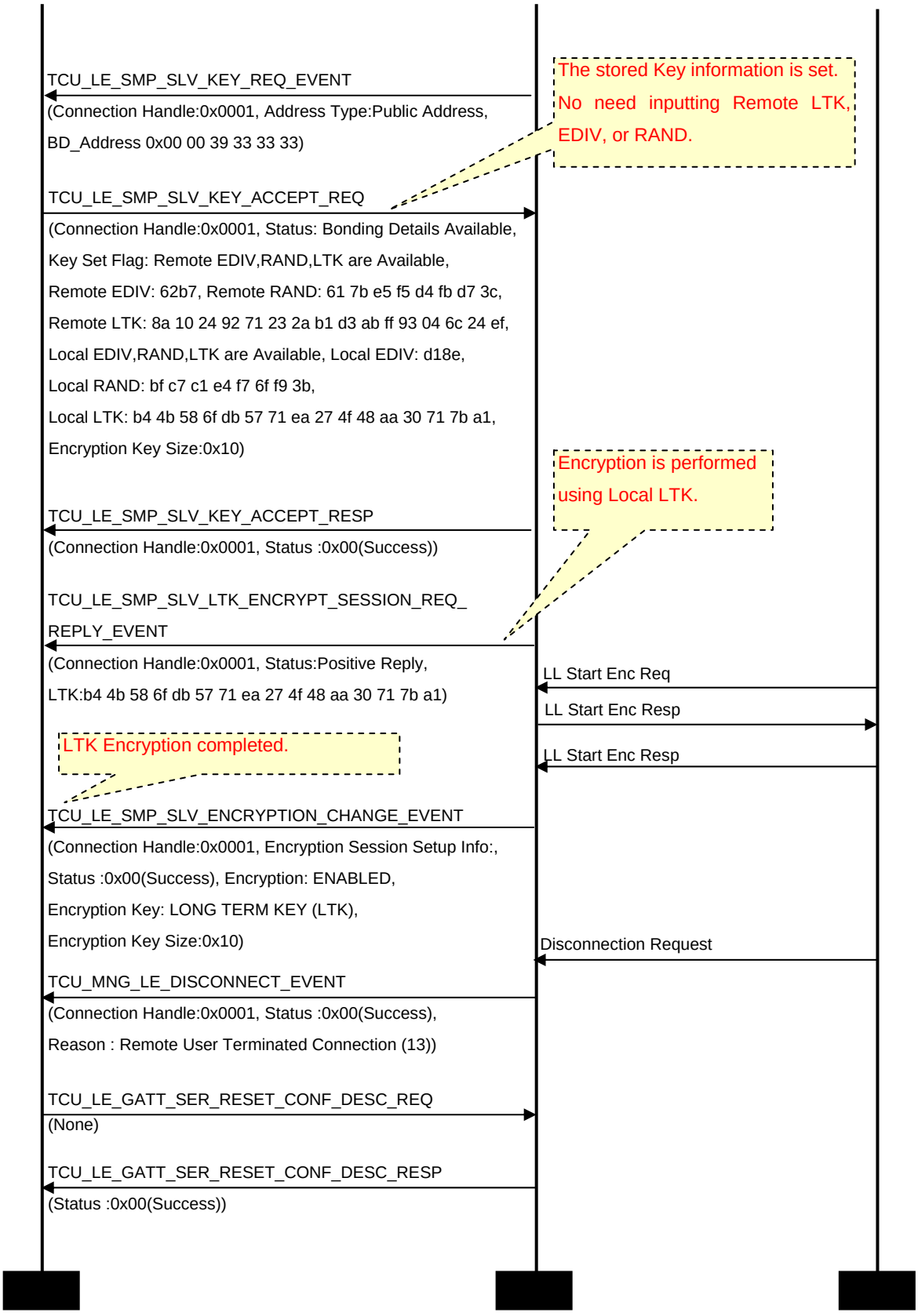
1.2 Connection -> Authentication(JustWork,LTK) from Central -> Disconnection -> Reconnection -> Encryption -> Disconnection



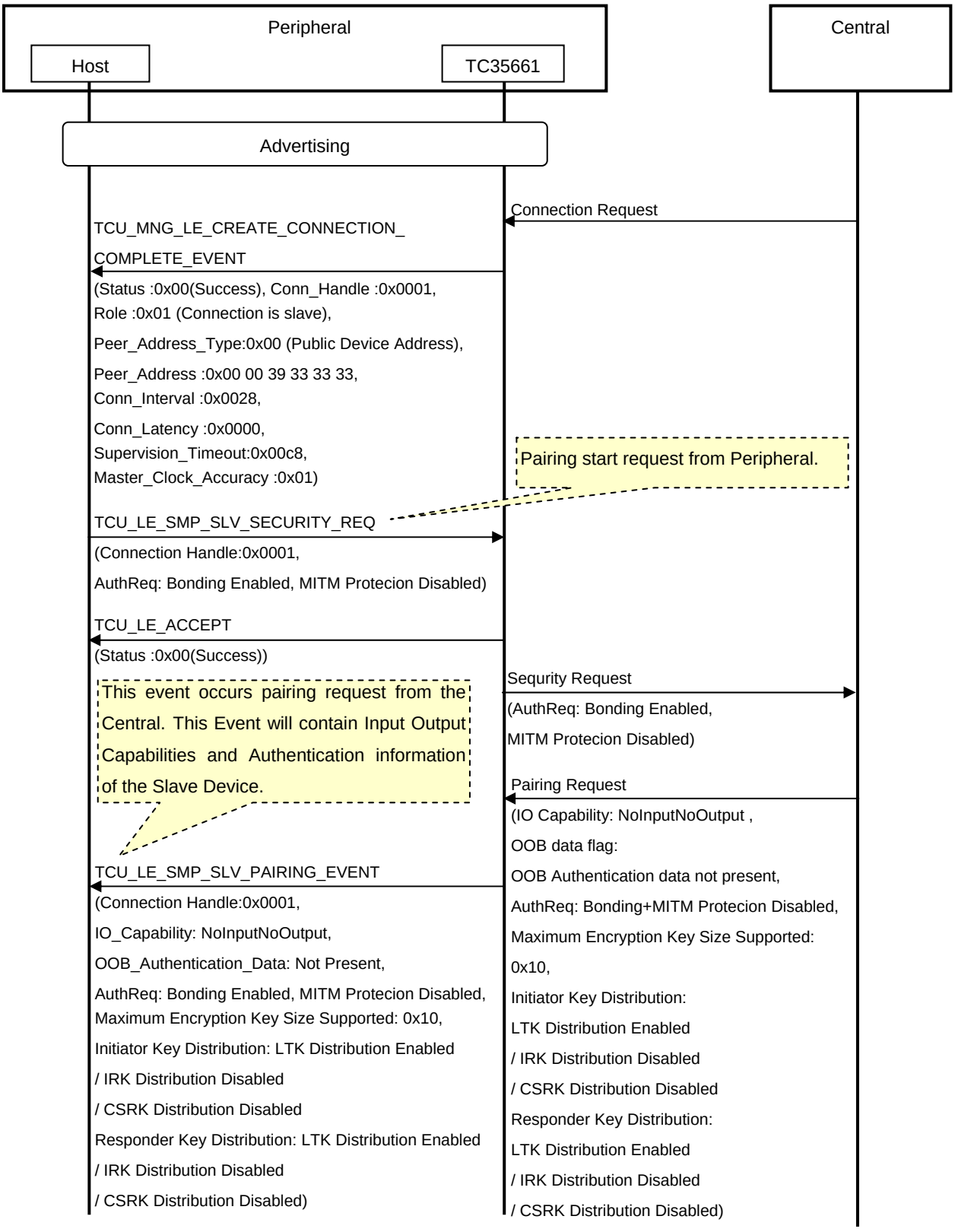

TCU_LE_SMP_SLV_PAIRING_ACCEPT_REQ
(Connection Handle:0x0001, Status :0x00(Success),
IO_Capability: NoInputNoOutput,
OOB_Authentication_Data: Not Present ,
AuthReq: Bonding Enabled, MITM Protecion Disabled,
Maximum Encryption Key Size Supported: 0x10,
Initiator Key Distribution: LTK Distribution Enabled
/ IRK Distribution Disabled / CSRK Distribution Disabled,
Responder Key Distribution: LTK Distribution Enabled
/ IRK Distribution Disabled / CSRK Distribution Disabled)
TCU_LE_ACCEPT
(Status :0x00(Success))
Pairing Response
(IO Capability: NoInputNoOutput ,
OOB data flag: OOB Authentication data not present,
AuthReq: Bonding+MITM Protecion Disabled,
Maximum Encryption Key Size Supported: 0x10,
Initiator Key Distribution: LTK Distribution Enabled
/ IRK Distribution Disabled / CSRK Distribution Disabled
Responder Key Distribution: LTK Distribution Enabled
/ IRK Distribution Disabled / CSRK Distribution Disabled)
TCU_LE_SMP_SLV_PAIRING_ACCEPT_RESP
(Connection Handle:0x0001, Status :0x00(Success))
TCU_LE_SMP_SLV_STK_GEN_METHOD_EVENT
(Connection Handle:0x0001, Status :0x00(Success),
STK GENERATION METHOD:
JUST WORK UNAUTHENTICATED)
PairingConfirm(Mconfirm)
PairingConfirm(Sconfirm)
ParingRandom(Mrand)
ParingRandom(Srand)
TCU_LE_SMP_SLV_STK_GENERATED_EVENT
(Connection Handle:0x0001
Short Term Key(STK):
b7 ff c2 16 28 c6 0e 4e 08 27 d8 1b 59 c7 c4 c9)
LL Enc Req
LL Enc Resp
TCU_LE_SMP_SLV_STK_ENCRYPT_SESSION_REQ_
REPLY_EVENT
(Connection Handle:0x0001, Status:Positive Reply,
STK: b7 ff c2 16 28 c6 0e 4e 08 27 d8 1b 59 c7 c4 c9)
LL Start Enc Req
LL Start Enc Resp
LL Start Enc Resp

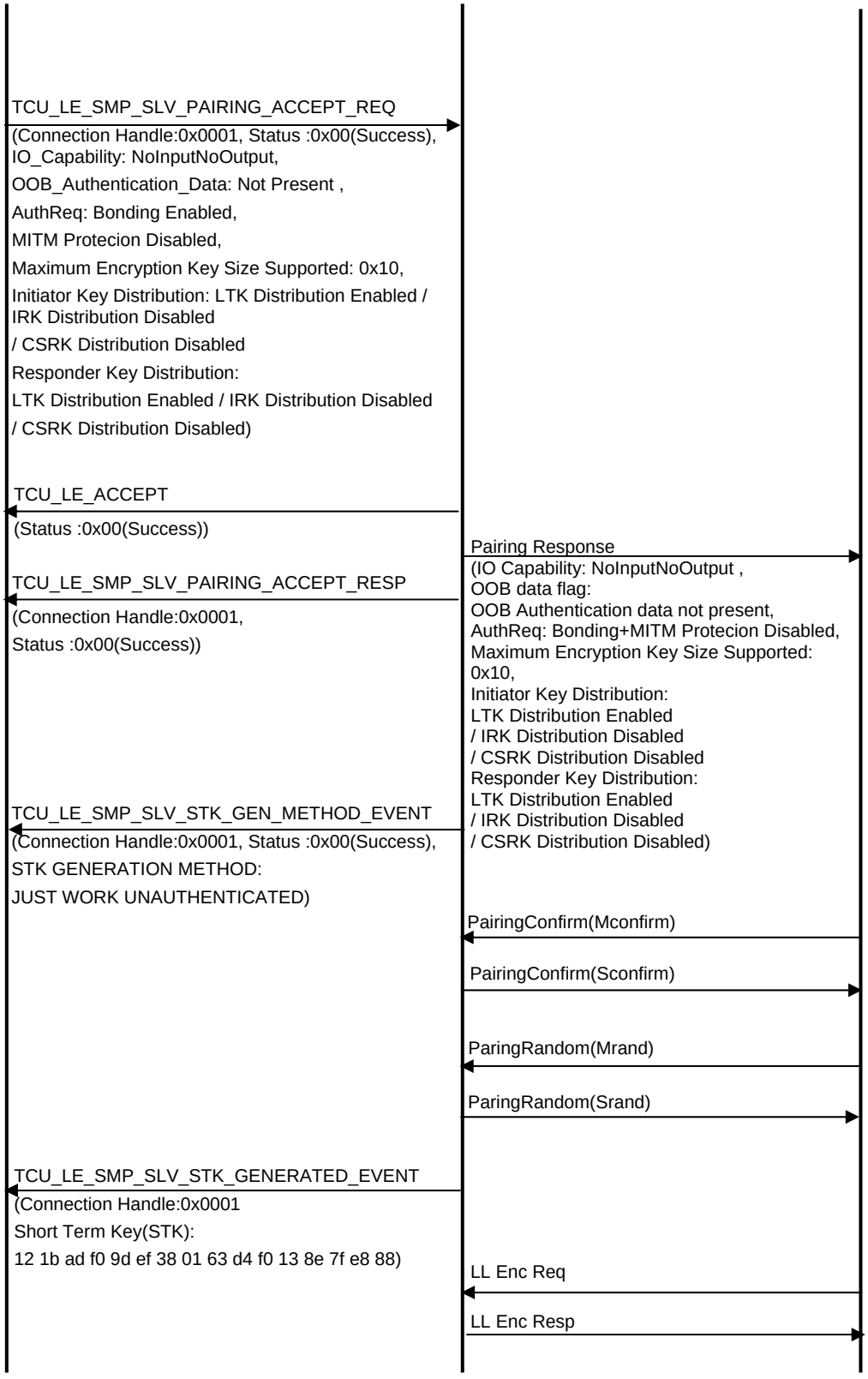

Host needs to save this LTK, EDIV, and RAND to EEPROM.
TCU_LE_SMP_SLV_ENCRYPTION_CHANGE_EVENT
(Connection Handle:0x0001,
Encryption Session Setup Info:,
Status :0x00(Success), Encryption: ENABLED,
Encryption Key: SHORT TERM KEY (STK),
Encryption Key Size:0x10)
Encryption Information
(Long Term Key:
b4 4b 58 6f db 57 71 ea 27 4f 48 aa 30 71 7b a1)
TCU_LE_SMP_SLV_LTK_SENT_EVENT
(Connection Handle:0x0001,
Long Term Key:
b4 4b 58 6f db 57 71 ea 27 4f 48 aa 30 71 7b a1)
Master Identification
(EDIV: d18e, RAND: bf c7 c1 e4 f7 6f f9 3b)
TCU_LE_SMP_SLV_EDIV_RAND_SENT_EVENT
(Connection Handle:0x0001,
EDIV: d18e, RAND: bf c7 c1 e4 f7 6f f9 3b)
Encryption Information
(Long Term Key:
8a 10 24 92 71 23 2a b1 d3 ab ff 93 04 6c 24 ef)
TCU_LE_SMP_SLV_LTK_RECEIVED_EVENT
(Connection Handle:0x0001,
Long Term Key(LTK):
8a 10 24 92 71 23 2a b1 d3 ab ff 93 04 6c 24 ef)
Master Identification
(EDIV: 62b7, RAND: 61 7b e5 f5 d4 fb d7 3c)
TCU_LE_SMP_SLV_EDIV_RAND_RECEIVED_EVENT
(Connection Handle:0x0001, EDIV: 62b7,
RAND: 61 7b e5 f5 d4 fb d7 3c)
TCU_LE_SMP_SLV_PAIRING_COMPLETED_EVENT
(Connection Handle:0x0001, Status :0x00(Success))
Key information is updated with this EVENT.
TCU_LE_SMP_SLV_STORE_KEY_EVENT
(Connection Handle:0x0001,
Address Type:Public Address,
Address 0x:00 00 39 33 33 33, Store Device Info)

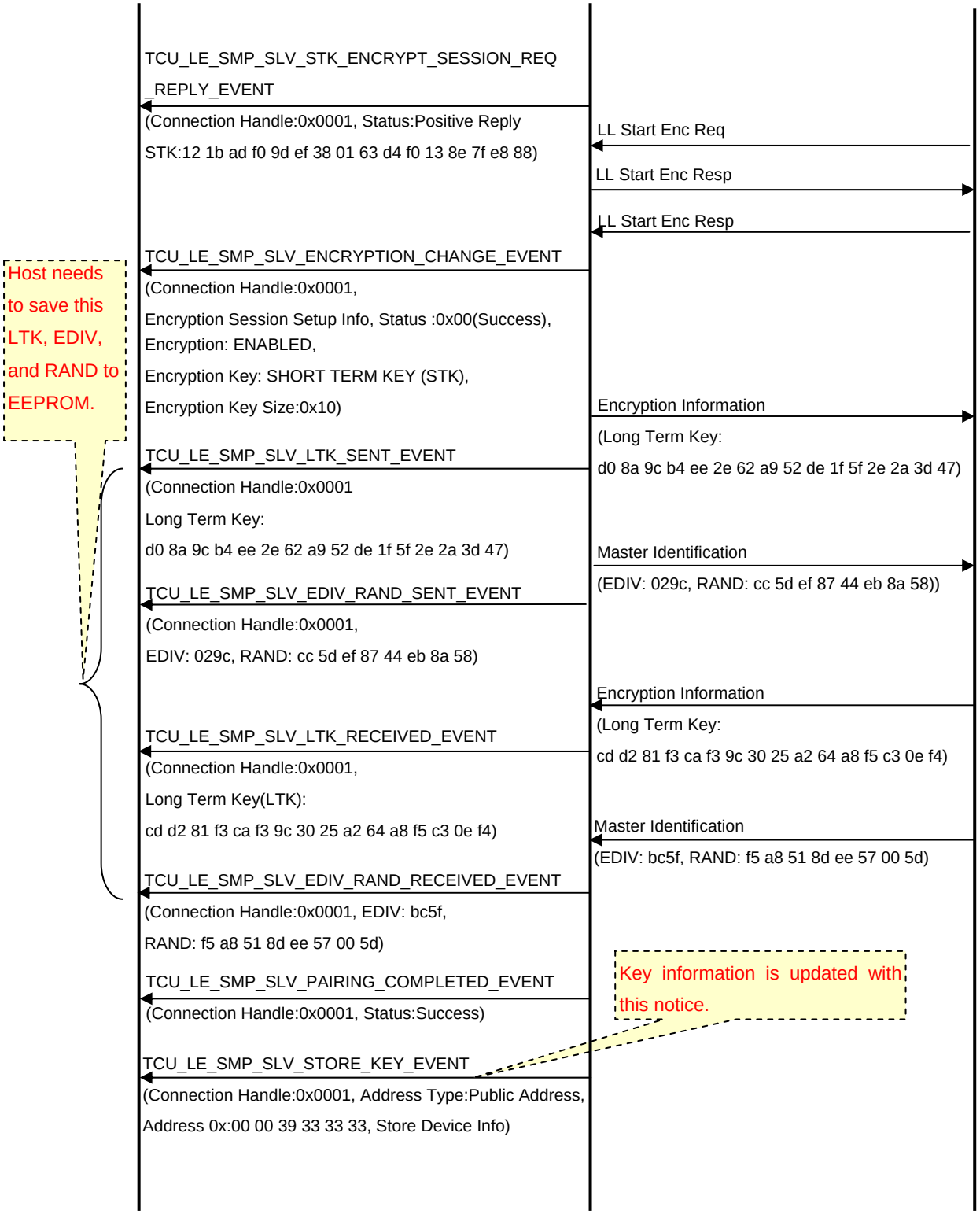

TCU_MNG_LE_DISCONNECT_REQ
(Remote device BD Address :0x00 00 39 33 33 33)
TCU_LE_ACCEPT
(Status :0x00(Success))
Disconnection Request
Disconnection Response
TCU_MNG_LE_DISCONNECT_EVENT
(Connection Handle:0x0001, Status :0x00(Success),
Reason : Connection Terminated By Local Host (16))
TCU_LE_GATT_SER_RESET_CONF_DESC_REQ
(None)
Advertising is necessary after disconnection.
TCU_LE_GATT_SER_RESET_CONF_DESC_RESP
(Status :0x00(Success))
Advertising
Connection Request
TCU_MNG_LE_CREATE_CONNECTION_COMPLETE_EVENT
(Status :0x00(Success), Conn_Handle :0x0001,
Role :0x01 (Connection is slave),
Peer_Address_Type:0x00 (Public Device Address),
Peer_Address :0x00 00 39 33 33 33, Conn_Interval :0x0028,
Conn_Latency :0x0000, Supervision_Timeout:0x00c8,
Master_Clock_Accuracy :0x01)
This command executes if connecting by ACL connection to an authenticated device.
TCU_SMP_LE_SLAVE_BONDING_ENABLED_INFO_REQ
(Connection Handle:0x0001)
TCU_LE_ACCEPT
(Status :0x00(Success))
Central Device Encryption Start
TCU_SMP_LE_SLAVE_BONDING_ENABLED_INFO_RESP
(Connection Handle:0x0001, Status :0x00(Success))
LL Enc Req
LL Enc Resp

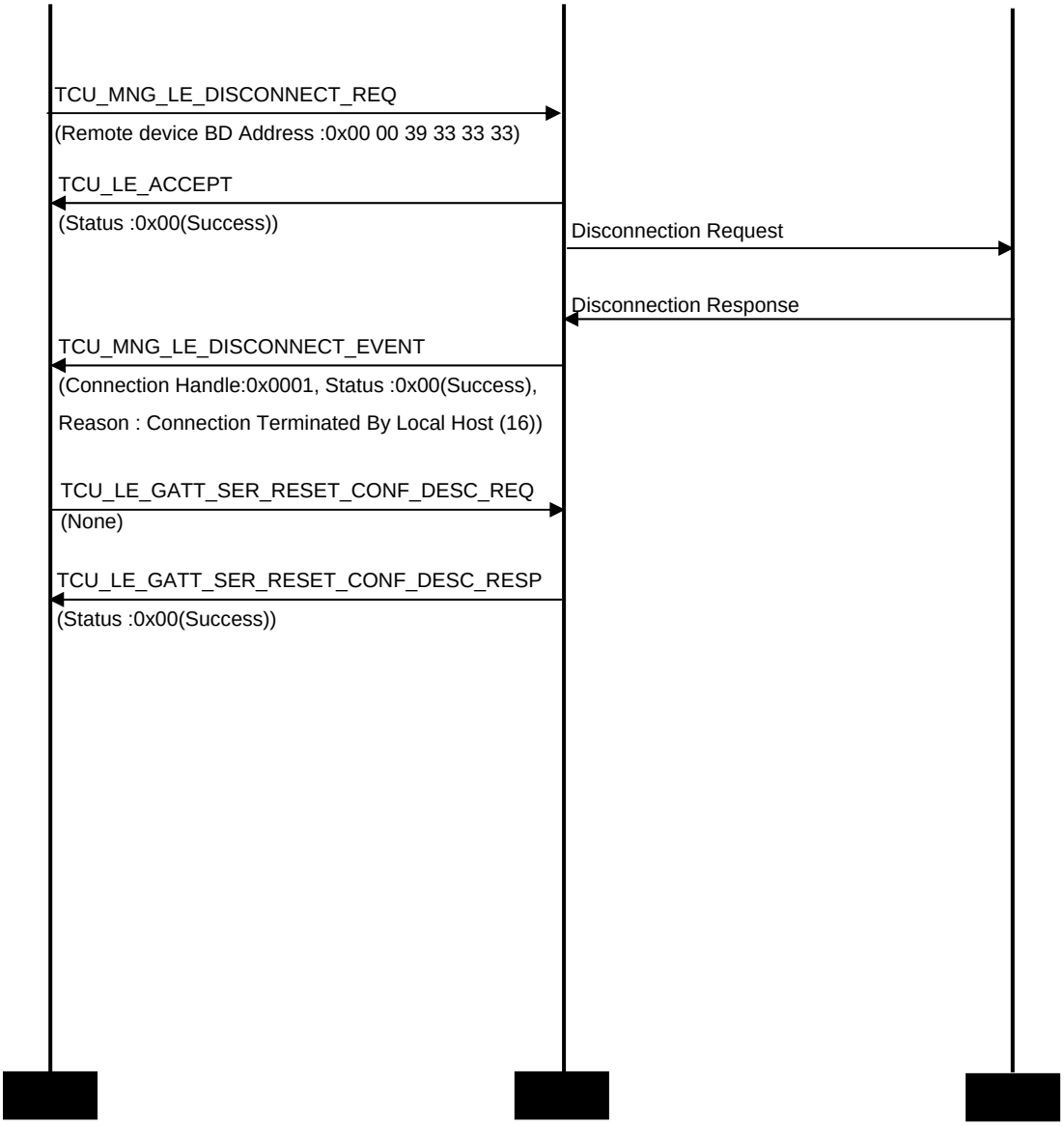

TCU_LE_SMP_SLV_KEY_REQ_EVENT
(Connection Handle:0x0001, Address Type:Public Address,
BD_Address 0x00 00 39 33 33 33)
The stored Key information is set.
No need inputting Remote LTK, EDIV, or RAND.
TCU_LE_SMP_SLV_KEY_ACCEPT_REQ
(Connection Handle:0x0001, Status: Bonding Details Available,
Key Set Flag: Remote EDIV,RAND,LTK are Available,
Remote EDIV: 62b7, Remote RAND: 61 7b e5 f5 d4 fb d7 3c,
Remote LTK: 8a 10 24 92 71 23 2a b1 d3 ab ff 93 04 6c 24 ef,
Local EDIV,RAND,LTK are Available, Local EDIV: d18e,
Local RAND: bf c7 c1 e4 f7 6f f9 3b,
Local LTK: b4 4b 58 6f db 57 71 ea 27 4f 48 aa 30 71 7b a1,
Encryption Key Size:0x10)
Encryption is performed using Local LTK.
TCU_LE_SMP_SLV_KEY_ACCEPT_RESP
(Connection Handle:0x0001, Status :0x00(Success))
TCU_LE_SMP_SLV_LTK_ENCRYPT_SESSION_REQ_
REPLY_EVENT
(Connection Handle:0x0001, Status:Positive Reply,
LTK:b4 4b 58 6f db 57 71 ea 27 4f 48 aa 30 71 7b a1)
LL Start Enc Req
LL Start Enc Resp
LL Start Enc Resp
LTK Encryption completed.
TCU_LE_SMP_SLV_ENCRYPTION_CHANGE_EVENT
(Connection Handle:0x0001, Encryption Session Setup Info:,
Status :0x00(Success), Encryption: ENABLED,
Encryption Key: LONG TERM KEY (LTK),
Encryption Key Size:0x10)
Disconnection Request
TCU_MNG_LE_DISCONNECT_EVENT
(Connection Handle:0x0001, Status :0x00(Success),
Reason : Remote User Terminated Connection (13))
TCU_LE_GATT_SER_RESET_CONF_DESC_REQ
(None)
TCU_LE_GATT_SER_RESET_CONF_DESC_RESP
(Status :0x00(Success))

1.3 Connection -> Authentication(JustWork,LTK) from Peripheral -> Disconnection

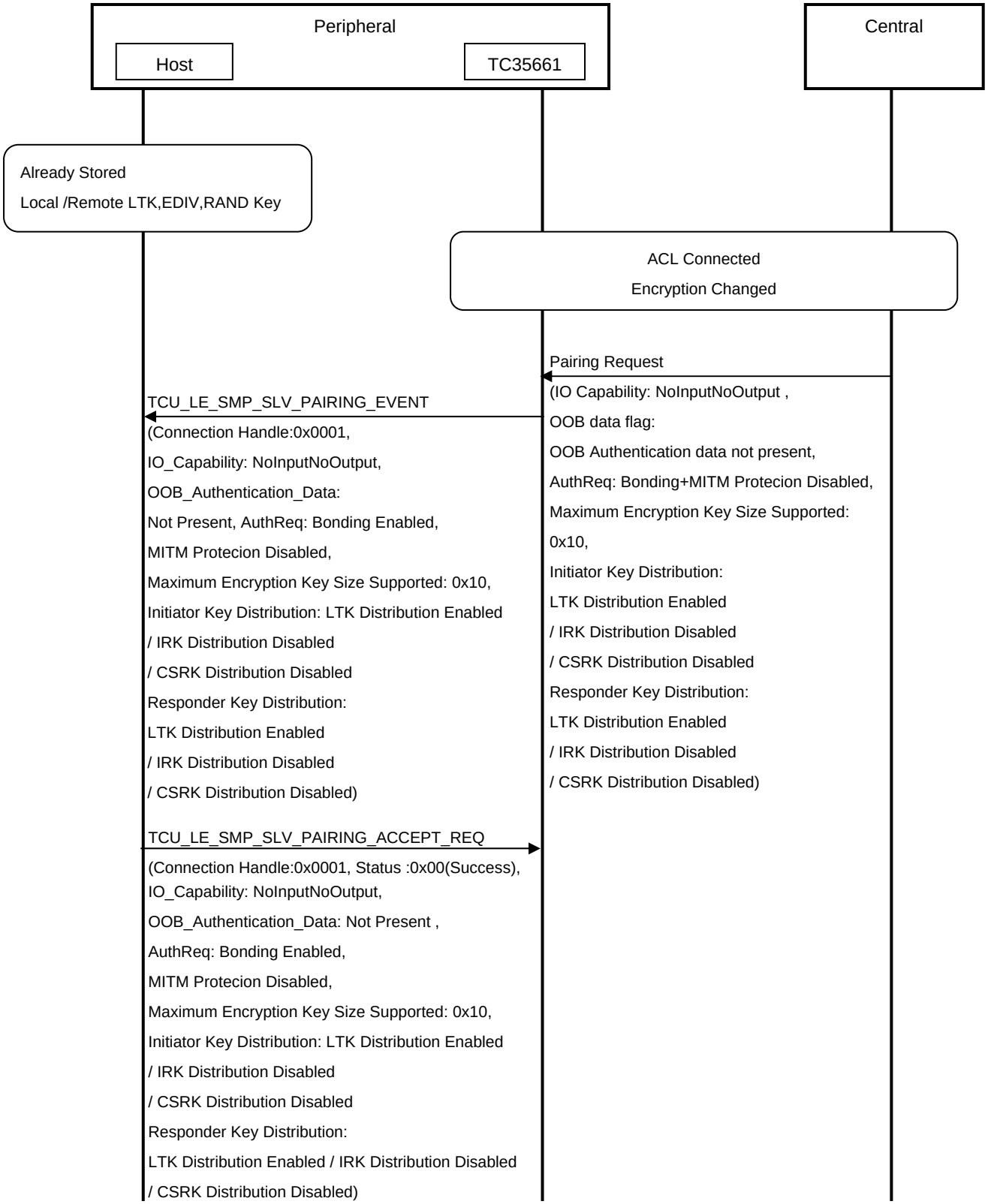


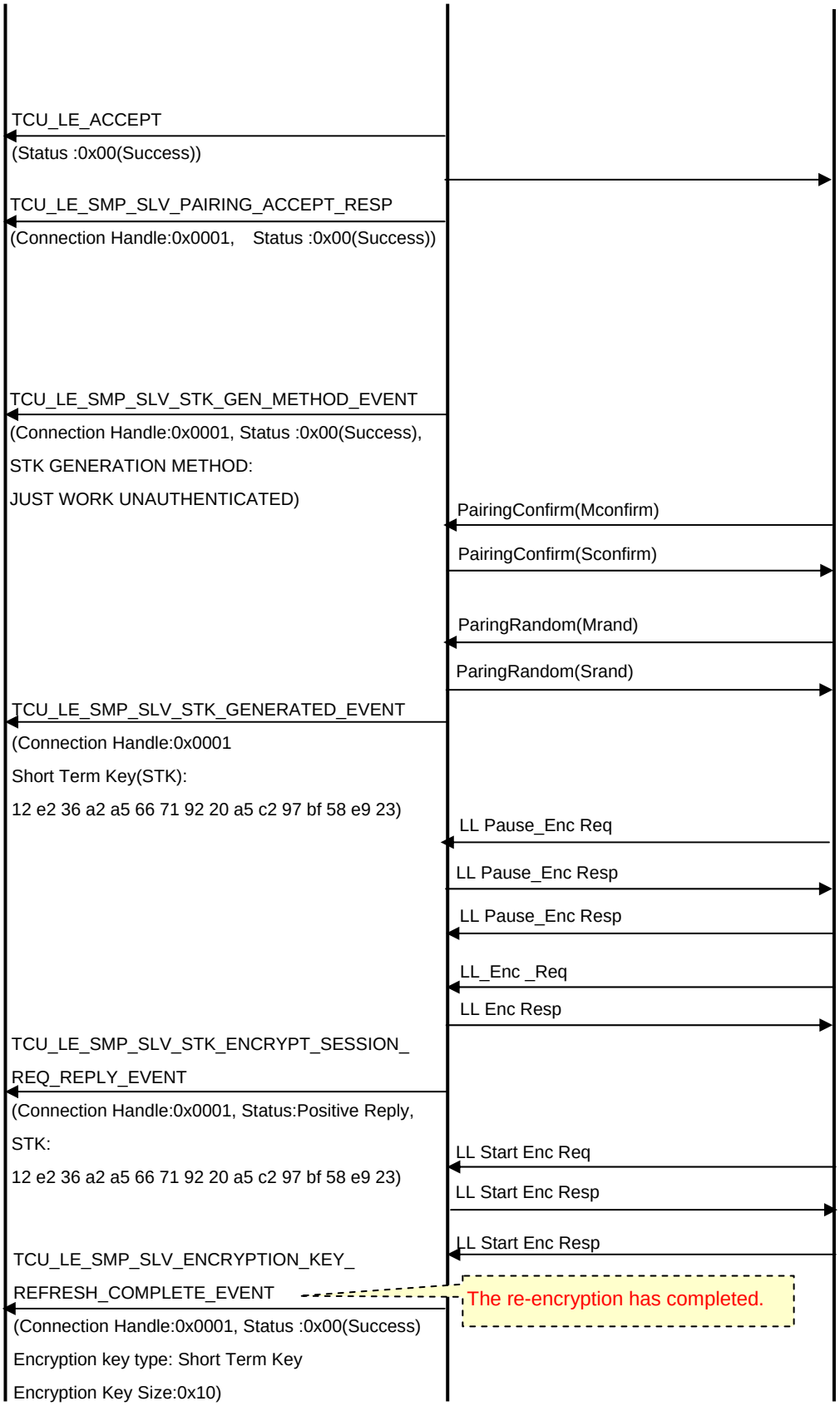

TCU_LE_SMP_SLV_PAIRING_ACCEPT_REQ
(Connection Handle:0x0001, Status :0x00(Success),
IO_Capability: NoInputNoOutput,
OOB_Authentication_Data: Not Present ,
AuthReq: Bonding Enabled,
MITM Protecion Disabled,
Maximum Encryption Key Size Supported: 0x10,
Initiator Key Distribution: LTK Distribution Enabled /
IRK Distribution Disabled
/ CSRK Distribution Disabled
Responder Key Distribution:
LTK Distribution Enabled / IRK Distribution Disabled
/ CSRK Distribution Disabled)
TCU_LE_ACCEPT
(Status :0x00(Success))
Pairing Response
(IO Capability: NoInputNoOutput ,
OOB data flag:
OOB Authentication data not present,
AuthReq: Bonding+MITM Protecion Disabled,
Maximum Encryption Key Size Supported:
0x10,
Initiator Key Distribution:
LTK Distribution Enabled
/ IRK Distribution Disabled
/ CSRK Distribution Disabled
Responder Key Distribution:
LTK Distribution Enabled
/ IRK Distribution Disabled
/ CSRK Distribution Disabled)
TCU_LE_SMP_SLV_PAIRING_ACCEPT_RESP
(Connection Handle:0x0001,
Status :0x00(Success))
TCU_LE_SMP_SLV_STK_GEN_METHOD_EVENT
(Connection Handle:0x0001, Status :0x00(Success),
STK GENERATION METHOD:
JUST WORK UNAUTHENTICATED)
PairingConfirm(Mconfirm)
PairingConfirm(Sconfirm)
ParingRandom(Mrand)
ParingRandom(Srand)
TCU_LE_SMP_SLV_STK_GENERATED_EVENT
(Connection Handle:0x0001
Short Term Key(STK):
12 1b ad f0 9d ef 38 01 63 d4 f0 13 8e 7f e8 88)
LL Enc Req
LL Enc Resp

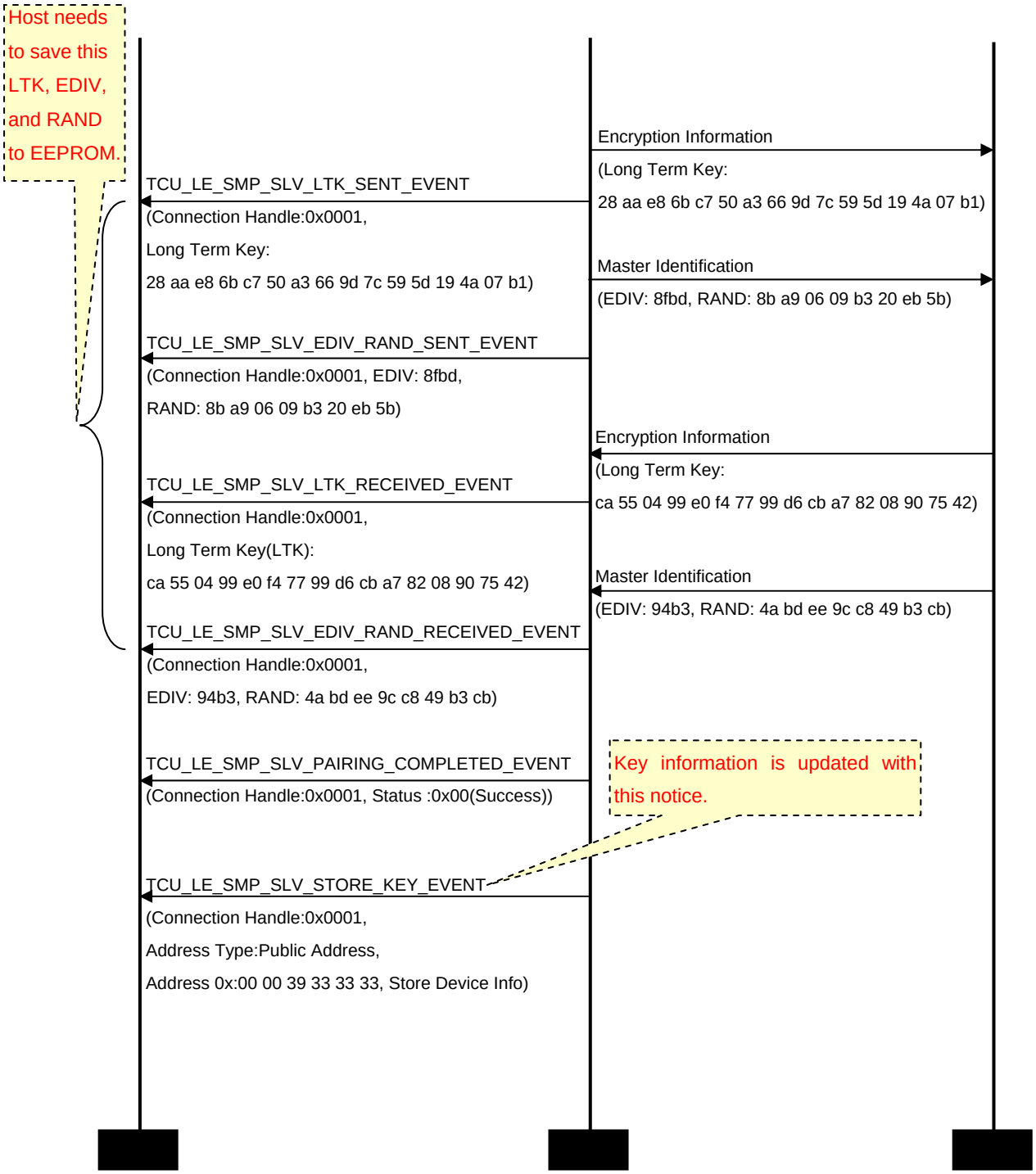

TCU_LE_SMP_SLV_STK_ENCRYPT_SESSION_REQ
_REPLY_EVENT
(Connection Handle:0x0001, Status:Positive Reply
STK:12 1b ad f0 9d ef 38 01 63 d4 f0 13 8e 7f e8 88)
LL Start Enc Req
LL Start Enc Resp
LL Start Enc Resp
TCU_LE_SMP_SLV_ENCRYPTION_CHANGE_EVENT
(Connection Handle:0x0001,
Encryption Session Setup Info, Status :0x00(Success),
Encryption: ENABLED,
Encryption Key: SHORT TERM KEY (STK),
Encryption Key Size:0x10)
Host needs to save this LTK, EDIV, and RAND to EEPROM.
Encryption Information
(Long Term Key:
d0 8a 9c b4 ee 2e 62 a9 52 de 1f 5f 2e 2a 3d 47)
TCU_LE_SMP_SLV_LTK_SENT_EVENT
(Connection Handle:0x0001
Long Term Key:
d0 8a 9c b4 ee 2e 62 a9 52 de 1f 5f 2e 2a 3d 47)
Master Identification
(EDIV: 029c, RAND: cc 5d ef 87 44 eb 8a 58))
TCU_LE_SMP_SLV_EDIV_RAND_SENT_EVENT
(Connection Handle:0x0001,
EDIV: 029c, RAND: cc 5d ef 87 44 eb 8a 58)
Encryption Information
(Long Term Key:
cd d2 81 f3 ca f3 9c 30 25 a2 64 a8 f5 c3 0e f4)
TCU_LE_SMP_SLV_LTK_RECEIVED_EVENT
(Connection Handle:0x0001,
Long Term Key(LTK):
cd d2 81 f3 ca f3 9c 30 25 a2 64 a8 f5 c3 0e f4)
Master Identification
(EDIV: bc5f, RAND: f5 a8 51 8d ee 57 00 5d)
TCU_LE_SMP_SLV_EDIV_RAND_RECEIVED_EVENT
(Connection Handle:0x0001, EDIV: bc5f,
RAND: f5 a8 51 8d ee 57 00 5d)
Key information is updated with this notice.
TCU_LE_SMP_SLV_PAIRING_COMPLETED_EVENT
(Connection Handle:0x0001, Status:Success)
TCU_LE_SMP_SLV_STORE_KEY_EVENT
(Connection Handle:0x0001, Address Type:Public Address,
Address 0x:00 00 39 33 33 33, Store Device Info)


TCU_MNG_LE_DISCONNECT_REQ
(Remote device BD Address :0x00 00 39 33 33 33)
TCU_LE_ACCEPT
(Status :0x00(Success))
Disconnection Request
Disconnection Response
TCU_MNG_LE_DISCONNECT_EVENT
(Connection Handle:0x0001, Status :0x00(Success),
Reason : Connection Terminated By Local Host (16))
TCU_LE_GATT_SER_RESET_CONF_DESC_REQ
(None)
TCU_LE_GATT_SER_RESET_CONF_DESC_RESP
(Status :0x00(Success))

1.4 Key update




TCU_LE_ACCEPT
(Status :0x00(Success))
TCU_LE_SMP_SLV_PAIRING_ACCEPT_RESP
(Connection Handle:0x0001, Status :0x00(Success))
TCU_LE_SMP_SLV_STK_GEN_METHOD_EVENT
(Connection Handle:0x0001, Status :0x00(Success),
STK GENERATION METHOD:
JUST WORK UNAUTHENTICATED)
PairingConfirm(Mconfirm)
PairingConfirm(Sconfirm)
ParingRandom(Mrand)
ParingRandom(Srand)
TCU_LE_SMP_SLV_STK_GENERATED_EVENT
(Connection Handle:0x0001
Short Term Key(STK):
12 e2 36 a2 a5 66 71 92 20 a5 c2 97 bf 58 e9 23)
LL Pause_Enc Req
LL Pause_Enc Resp
LL Pause_Enc Resp
LL_Enc _Req
LL Enc Resp
TCU_LE_SMP_SLV_STK_ENCRYPT_SESSION_
REQ_REPLY_EVENT
(Connection Handle:0x0001, Status:Positive Reply,
STK:
12 e2 36 a2 a5 66 71 92 20 a5 c2 97 bf 58 e9 23)
LL Start Enc Req
LL Start Enc Resp
LL Start Enc Resp
TCU_LE_SMP_SLV_ENCRYPTION_KEY_
REFRESH_COMPLETE_EVENT
The re-encryption has completed.
(Connection Handle:0x0001, Status :0x00(Success)
Encryption key type: Short Term Key
Encryption Key Size:0x10)



End of document.