Bluetooth Baseband LSI

Panasonic PAN1026

Toshiba TC35661

SMP

Command Interface Document

July.2013

Revision History

Date	Modification	Note
24th-June-2013	1st Release Based on TC35661APL_ROM500_SMP_SDS_E_12thJune2013	

26th-July-2013	Added new section "4 LIST OF ERROR CODES"
	
	Added new command
	"TCU_LE_SMP_SLV_ENCRYPTION_KEY_REFRESH_COMPLETE_EVENT"
	
	Changed OpCode of the following commands
	  1.5 TCU_LE_SMP_SLV_PAIRING_FAILED_REQ
	  1.25 TCU_LE_SMP_SLV_IRK_RECEIVED_EVENT
	  1.26 TCU_LE_SMP_SLV_IDENTITY_ADDRESS_RECEIVED_EVENT
	  1.27 TCU_LE_SMP_SLV_CSRK_RECEIVED_EVENT
	  1.28 TCU_LE_SMP_SLV_IRK_SENT_EVENT
	  1.29 TCU_LE_SMP_SLV_IDENTITY_ADDRESS_SENT_EVENT
	  1.30 TCU_LE_SMP_SLV_CSRK_SENT_EVENT
	Changed ServiceID of the following commands
	  1.30 TCU_LE_SMP_SLV_CSRK_SENT_EVENT
	Fixed Typos.	

Contents

1   Command Format for LE SM Module

For All SMP TCU Commands Data input (Param Len, Conn Handle etc) must be in Little Endian Format. Also the data output through Response and Event will be in Little Endian Format.

For each Request, Response and Event that is sent to remote device "Connection Handle" is added as the parameter. "Connection Handle" is used as the index for accessing the remote device. This is needed to support Multiple Instances for SM module.

1.1 TCU_LE_SMP_SLV_PAIRING_EVENT

This event is generated by Slave Device to inform the Application that a Pairing Request has been received from the Master Device. In response to this event, Slave application will generate the Slave Pairing Accept Request **"TCU_LE_SMP_SLV_PAIRING_ACCEPT_REQ"**. This Event will contain Input Output Capabilities and Authentication information of the Slave Device.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
IO_Capability	1 Byte
OOB_Data_Flag	1 Byte
Auth_Req	1 Byte
Max_Enc_Key_Size	1 Byte
Init_Key_Dist	1 Byte
Resp_Key_Dist	1 Byte

ServiceID   0xD5
OpCode   0xC1
Parameter Length   0x0008

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
IO_Capability	Defines the Input Output capabilities of the device. DisplayOnly DisplayYesNo KeyboardOnly NoInputNoOutput KeyboardDisplay	 0x00 0x01 0x02 0x03 0x04
OOB_Data_Flag	Indicates whether OOB authentication data is available OOB data not present OOB data present	 0x00 0x01
Auth_Req	Indicates the requested security properties	0x00 – 0x05 (Refer [2.1 AUTH_REQ])
Max_Enc_Key_Size	Defines the maximum encryption key size in octets that the device can support.	7-16
Init_Key_Dist	Indicates which keys the initiator is requesting to distribute or use during the Transport Specific Key Distribution Phase	0 – 7(Refer [2.2 INIT_KEY_DIST AND RESP_KEY_DIST])
Resp_Key_Dist	The Responder Key Distribution field indicates which keys the initiator is requesting the responder to distribute or use during the Transport Specific Key Distribution phase	0 – 7(Refer [2.2 INIT_KEY_DIST AND RESP_KEY_DIST])

1.2   TCU_LE_SMP_SLV_PAIRING_ACCEPT_REQ

The Accept Request is generated by Slave application in response to Pairing Event. The Slave application will respond with its Authentication Requirements or Error Code if pairing is not supported. The TCU_LE_ACCEPT is sent to Slave Application when this request is received by the Slave Device. The Slave Device will indicate this pairing response to the Master Device.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Status	1 Byte
IO_Capability	1 Byte
OOB_Data_Flag	1 Byte
Auth_Req	1 Byte
Max_Enc_Key_Size	1 Byte
Init_Key_Dist	1 Byte
Resp_Key_Dist	1 Byte

ServiceID   0xD5
OpCode   0x01
Parameter Length   0x0003 -0x0009

Parameters

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Status	On Success pairing response is sent by Slave device providing IO capabilities and Authentication Requirements. On Failure the Pairing Failed Command Error will be sent by slave device with appropriate error code and no other data will be sent. - Success - Refer Error Code table	 0x00 --- .
IO_Capability	Defines the Input Output capabilities of the device. - DisplayOnly - DisplayYesNo - KeyboardOnly - NoInputNoOutput - KeyboardDisplay	 0x00 0x01 0x02 0x03 0x04
OOB_Data_Flag	Indicates whether OOB authentication data is available - OOB data not present - OOB ata present	 0x00 (OOB data not present) 0x01 (OOB Data Present)
Auth_Req	Indicates the requested security properties	0x00 – 0x05 (Refer [2.1 AUTH_REQ])
Max_Enc_Key_Size	Defines the maximum encryption key size in octets that the device can support.	7-16
Init_Key_Dist	Indicates which keys the initiator is requesting to distribute or use during the Transport Specific Key Distribution Phase	0 – 7(Refer [2.2 INIT_KEY_DIST AND RESP_KEY_DIST])
Resp_Key_Dist	The Responder Key Distribution field indicates which keys the initiator is requesting the responder to distribute or use during the Transport Specific Key Distribution phase	0 – 7(Refer [2.2 INIT_KEY_DIST AND RESP_KEY_DIST])

1.3 TCU_LE_SMP_SLV_PAIRING_ACCEPT_RESP

This response is sent to Slave Application by Slave Device on receiving the Accept Request from Slave Application. Once the Slave Device responds to the Master Device this response is generated.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Status	1 Byte

ServiceID   0xD5
OpCode   0x81
Parameter Length   0x0003

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Status	Result Code: - Success - Refer Error Code table	0x00 ---

1.4 TCU_LE_SMP_SLV_SECURITY_REQ

This request is generated by the Slave Application to the Slave Device to request the Master to initiate the pairing process. Once the processing of this request is started **TCU_LE_ACCEPT** is received by the Slave. Once the Master initiates the pairing process the **"TCU_LE_SMP_SLV_PAIRING_EVENT"** will be generated by Slave Device to the application.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Auth_Req	1 Byte

ServiceID	0xD5
OpCode	0x02
Parameter Length	0x0003

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Auth_Req	Indicates the requested security properties	0x00 – 0x05 (Refer [2.1 AUTH_REQ])

1.5   TCU_LE_SMP_SLV_PAIRING_FAILED_REQ

This command is issued by the Slave Device when the user wishes to abort the pairing process. This is an asynchronous command that can be sent at any time during the pairing process.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Reason	1 Byte

ServiceID   0xD5
OpCode   0x13
Parameter Length   0x0003

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Reason	When pairing process fails the result code is sent indicating the cause for the failure.	Refer Error Code table

1.6   TCU_LE_SMP_SLV_PAIRING_FAILED_RESP

This response is issued by the Slave Device after the processing of the request "TCU_LE_SMP_SLV_ PAIRING_FAILED_REQ".

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Reason	1 Byte

ServiceID   0xD5
OpCode   0x53
Parameter Length   0x0003

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Reason	The reason to abort pairing process.	Refer Error Code table

1.7 TCU_LE_SMP_SLV_PAIRING_FAILED_EVENT

This event is generated by the Slave Device to the application when pairing process results in the failure.
This is an asynchronous event that can be sent at any time during the pairing process.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Reason	1 Byte

ServiceID   0xD5
OpCode   0x43
Parameter Length   0x0003

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Reason	When pairing process fails the result code is sent indicating the cause for the failure.	Refer Error Code table

1.8   TCU_LE_SMP_SLV_STK_GEN_METHOD_EVENT

This event is generated by the Slave Device to the Application to indicate the method selected to generate the Short Term Key (STK). The STK generation method is selected based on parameters (I/O Capability, OOB Data Flag, Auth_Req Flag) of the pairing response sent by the slave device.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Status	1 Byte
STK Generation Method	1 Byte

ServiceID   0xD5
OpCode   0xCB
Parameter Length   0x0004

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Status	Result Code: Success Key Entry Failed	0x00 0x01
STK Generation Method	Method selected to generate the Short Term Key(STK) JUST WORK UNAUTHENTICATED PASSLEY ENTRY ;Initialtor Displays, Responder Inputs Authenticated PASSKEY ENTRY: Initiator Inputs, Responder Displays Authenticated. PASSKEY ENTRY: Initiator and Responder inputs Authenticated.	 0x00 0x01 0x02 . 0x03

1.9   TCU_LE_SMP_SLV_KEY_ENTRY_REQ_EVENT

This command is sent by the Slave Device to the application to request to enter the PassKey used in the **"PassKey Entry"** Pairing method. This event is generated as part of pairing process. In response to this event, the application will generate the **"TCU_LE_SMP_SLV_KEY_ENTRY_WRITE_REQ"** the key write request to input the Passkey.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes

ServiceID   0xD5
OpCode   0x44
Parameter Length   0x0002

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)

1.10 TCU_LE_SMP_SLV_KEY_ENTRY_WRITE_REQ

This request contains the key entered by the Slave Device which is used to generate the PassKey used in the **"PassKey Entry"** Pairing method. This request is generated by the application to Slave Device to input/write the key needed for pairing process.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Status	1 Byte
Key	3 Bytes

ServiceID   0xD5
OpCode: 0x05
Parameter Length   0x0003 or 0x0006

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Status	Result Code: Success Key Entry Failed	0x00 0x01
Key	6 numeric digits which will contained when Status is success i.e. when key is entered through Keyboard Input successfully.	000000 to 999999

1.11   TCU_LE_SMP_SLV_KEY_ENTRY_WRITE_RESP

This response is generated by the Slave Device to the Application in response to key write entry request "TCU_LE_SMP_SLV_KEY_ENTRY_WRITE_REQ".

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Status	1 Byte

ServiceID   0xD5
OpCode   0x85
Parameter Length   0x0003

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Status	Result Code: - Success - Refer Error Code table	0x00 ---

1.12 TCU_LE_SMP_SLV_DISPLAY_KEY_EVENT

This event is sent by the Slave Device to its application to input the passkey displayed on the LE Device. This PassKey is used in the **"PassKey Entry"** Pairing method. This event is generated as part of pairing process. In response to this event, the application will generate the **"TCU_LE_SMP_SLV_DISPLAY_KEY_WRITE_REQ"** the key write request to input the Displayed Key.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes

ServiceID   0xD5
OpCode   0x46
Parameter Length 0x0002

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)

1.13 TCU_LE_SMP_SLV_DISPLAY_KEY_WRITE_REQ

This request contains the key displayed by the Slave Device which is used to generate the PassKey used in the **"PassKey Entry"** Pairing method. This request is generated by the application to Slave Device to input/write the key displayed on the device which is needed for pairing process.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Status	1 Byte
Key	3 Bytes

ServiceID   0xD5
OpCode   0x07
Parameter Length   0x0003 or 0x0006

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Status	Result Code: Success Key Entry Failed	0x00 0x01
Key	6 numeric digits which will contained when Status is success i.e. when key is entered through Keyboard Input successfully.	000000 to 999999

1.14   TCU_LE_SMP_SLV_DISPLAY_KEY_WRITE_RESP

This response is generated by the Slave Device to the Application in response to display key write request
"TCU_LE_SMP_SLV_DISPLAY_KEY_WRITE_REQ".

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Status	1 Byte

ServiceID   0xD5
OpCode   0x87
Parameter Length   0x0003

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Status	Result Code: - Success - Refer Error Code table	0x00 ---

1.15   TCU_LE_SMP_SLV_STK_GENERATED_EVENT

This event indicates the short term key is successfully generated in pairing process (Phase 2).This Event is generated by the Slave Device to the Application to help track the status of pairing process.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Short Term Key	16 Bytes

ServiceID   0xD5
OpCode   0x48
Parameter Length   0x0012

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Short Term Key	Short Tem Key	128 bits

1.16   TCU_LE_SMP_SLV_LTK_RECEIVED_EVENT

This event is generated by Slave Device to Application, when it receives the LTK key from the Master Device (Phase3). This event is generated to track the progress of pairing process for the Slave Application.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Long Term Key	16 Byte

ServiceID   0xD5
OpCode   0xC9
Parameter Length   0x0012

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Long Term Key	Long Tem Key	128 bits

1.17 TCU_LE_SMP_SLV_EDIV_RAND_RECEIVED_EVENT

This event is generated by Slave Device to Application, when it receives the EDIV and RAND values from the Master Device (Phase3). This event is generated to track the progress of pairing process for the Slave Application.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
EDIV	2 Bytes
RAND	8 Bytes

ServiceID   0xD5
OpCode   0xCA
Parameter Length   0x000C

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
EDIV	Encrypted Diversifier Value received from the Master device.	16 bits
RAND	Random Number received from the MAster device.	8 bytes

1.18   TCU_LE_SMP_SLV_LTK_SENT_EVENT

This event is generated by Slave Device to Application, when the Slave device sends the LTK key to the Master device. This event is generated to track the progress of pairing process for the Slave Application.. This event is generated only if **EncKey** is set to 1 in **Responder Key Distribution** field (**Refer to Section 3.6.1, Page 628 of Core Spec V4.0**) of Pairing Response sent by the slave device.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Long Term Key	16 Bytes

ServiceID   0xD5
OpCode   0xCC
Parameter Length   0x0012

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Long Term Key	Long Tem Key	128 bits

1.19   TCU_LE_SMP_SLV_EDIV_RAND_SENT_EVENT

This event is generated by Slave Device to Application, when the Slave device sends the EDIV and RAND values to the Master device. This event is generated to track the progress of pairing process for the Slave Application.. This event is generated only if **EncKey** is set to 1 in **Responder Key Distribution** field (**Refer to Section 3.6.1, Page 628 of Core Spec V4.0**) of Pairing Response sent by the slave device.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
EDIV	2 Bytes
RAND	8 Bytes

ServiceID   0xD5
OpCode   0xCD
Parameter Length   0x000C

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
EDIV	Encrypted Diversifier Value received from the slave device.	16 bits
RAND	Random Number received from the slave device.	8 bytes

1.20   TCU_LE_SMP_SLV_ENCRYPTION_CHANGE_EVENT

This event is generated by Slave Device to Application. This event indicates that the, encryption session is setup i.e. link is encrypted. This event also indicates whether the session is encrypted using **Short Term Key** (in Pahse2 to distribute the Transport Specific keys) or with the **Long Term Key**.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Status	1 Byte
Key Type	1 Byte
Encryption Flag	1 Byte
Encryption_Key_Size	1 Byte

ServiceID   0xD5
OpCode   0xD0
Parameter Length   0x0006

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Status	Result Code: Success - Refer Error Code table	0x00 ---
Key Type	Key Type indicates whether the session is encrypted using Short Term Key (in Pahse2 to distribute the Transport Specific keys) or with the Long Term Key Short Term Key(STK) Long Term Key(LTK)	 0x01 0x02
Encryption Flag	Encryption Flag indicates whether link is encrypted or not Encryption enabled Encryption disabled	 0x00 0x01
Encryption Key Size	Encryption Key Size Value negotiated between Bonded Devices	7-16

1.21   TCU_LE_SMP_SLV_ENCRYPTION_KEY_REFRESH_COMPLETE_EVENT

This event is generated by Slave Device to Application. This event indicates that the, encryption session is setup i.e. link is encrypted. The Encryption Key Refresh Complete event is used to indicate to the encryption key was refreshed on the given Connection_Handle any time encryption is paused and then resumed. This event also indicates whether the session is encrypted using Short Term Key (in Pahse2 to distribute the Transport Specific keys) or with the Long Term Key (After Phase 3 using HCI Start Encrypt Command by the Host).

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Status	1 Byte
Key Type	1 Byte
Encryption_Key_Size	1 Byte

ServiceID   0xD5
OpCode   0xD1
Parameter Length   0x0005

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Status	Result Code: -Success - Refer Error Code table	0x00 ----
Key Type	Key Type indicates whether the session is encrypted using Short Term Key (in Pahse2 to distribute the Transport Specific keys) or with the Long Term Key (After Phase 3 HCI Start Encrypt Command).	0x01 – Short Term Key (STK) 0x02 – Long Term Key (LTK)
Encryption Key Size	Encryption Key Size Value negotiated between Bonded Devices.	7-16

1.22 TCU_LE_SMP_SLV_PAIRING_COMPLETED_EVENT

This event is generated by Slave Device to Application. This event indicates that the, paring process has been completed.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Status	1 Byte

ServiceID   0xD5
OpCode   0xD2
Parameter Length   0x0003

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Status	Result Code: Success Failed	0x00 0x01

1.23   TCU_LE_SMP_SLV_STK_ENCRYPT_SESSION_REQ_REPLY_EVENT

This event is generated by Slave Device to Application. This event is generated by the slave device when it sends the Long Term Key Request Reply to the Master Device on receiving the LE Long Term Key Request Event.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Status	1 Byte
STK	16 Bytes

ServiceID   0xD5
OpCode   0xCE
Parameter Length   0x0003 or 0x0013

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Status	Result Code: Success Failure	0x00 – Positive Reply 0x01 – Negative Reply
STK	Short Term Key Replied by the salve device to the Master device for encrypting the link.	16 bytes

1.24 TCU_LE_SMP_SLV_LTK_ENCRYPT_SESSION_REQ_REPLY_EVENT

This event is generated by Slave Device to Application. This event is generated by the slave device when it sends the Long Term Key Request Reply to the Master Device on receiving the LE Long Term Key Request Event.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Status	1 Byte
LTK	16 Bytes

ServiceID   0xD5
OpCode   0xCF
Parameter Length   0x0003 or 0x0013

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Status	Result Code: Success Failure	0x00 – Positive Reply 0x01 – Negative Reply
LTK	Long Term Key Replied by the salve device to the Master device for encrypting the link.	16 bytes

1.25 TCU_LE_SMP_SLV_IRK_RECEIVED_EVENT

This event is generated by Slave Device to Application, when it receives the IRK key from the Master Device (Phase3). This event is generated to track the progress of pairing process for the Slave Application.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
IRK	16 Bytes

ServiceID   0xD5
OpCode   0xD6
Parameter Length   0x0012

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
IRK	This Identity Resolving Key received from the Peer Device is used to resolve the Resolvable Private Address of the Peer Device.	16 Bytes

1.26 TCU_LE_SMP_SLV_IDENTITY_ADDRESS_RECEIVED_EVENT

This event is generated by Slave Device to Application, when it receives the Identity Address Information from the Master Device (Phase3). This event is generated to track the progress of pairing process for the Slave Application.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Address_Type	1 Byte
Identity_Address	6 Bytes

ServiceID   0xD5
OpCode   0xD7
Parameter Length   0x0009

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Address_Type	Indicates the type of the Identity Address received. Public Address Random Address	 0x00 0x01
Identity Address	Device Address	0xXXXXXXXXXXXX

1.27 TCU_LE_SMP_SLV_CSRK_RECEIVED_EVENT

This event is generated by Slave Device to Application, when it receives the CSRK key from the Master Device (Phase3). This event is generated to track the progress of pairing process for the Slave Application.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
CSRK	16 Bytes

ServiceID   0xD5
OpCode   0xD8
Parameter Length   0x0012

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
CSRK	This Connection Signature Resolving Key from the Peer Device is used for Verifying the Signed Data from the Peer Device.	16 Bytes

1.28 TCU_LE_SMP_SLV_IRK_SENT_EVENT

This event is generated by Slave Device to Application, when it sends the IRK to the slave device. This event is generated to track the progress of pairing process for the Slave Application. This event is generated only if **IdKey** bit is set to 1 in **Initiator Key Distribution** field (**Refer to Section 3.6.1, Page 628 of Core Spec V4.0**) of Pairing Event Received (**TCU_LE_SMP_SLV_PAIRING_ACCEPT_REQ**) from the slave device.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
IRK	16 Bytes

ServiceID   0xD5
OpCode   0xD3
Parameter Length   0x0012

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
IRK	This Local Identity Resolving Key is used to generate the Resolvable Private Address for the Device.	16 Bytes

1.29   TCU_LE_SMP_SLV_IDENTITY_ADDRESS_SENT_EVENT

This event is generated by Slave Device to Application, when it sends the Identity Address to the Master Device. This event is generated to track the progress of pairing process for the Slave Application. This event is generated only if **IdKey** bit is set to 1 in **Initiator Key Distribution** field (**Refer to Section 3.6.1, Page 628 of Core Spec V4.0**) of Pairing Event Received (**TCU_LE_SMP_SLV_PAIRING_ACCEPT_REQ**) from the slave device.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Address Type	1 Byte
Identity Address	6 Bytes

ServiceID   0xD5
OpCode   0xD4
Parameter Length   0x0009

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Address_Type	Indicates the type of the Identity Address received. Public Address Random Address	 0x00 0x01
Identity Address	Device Address	0xXXXXXXXXXXXX

1.30 TCU_LE_SMP_SLV_CSRK_SENT_EVENT

This event is generated by Slave Device to Application, when it sends the CSRK to the slave device. This event is generated to track the progress of pairing process for the Slave Application. This event is generated only if **Sign** bit is set to 1 in **Initiator Key Distribution** field (**Refer to Section 3.6.1, Page 628 of Core Spec V4.0**) of Pairing Event Received (**TCU_LE_SMP_SLV_PAIRING_ACCEPT_REQ**) from the slave device.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
CSRK	16 Byte

ServiceID   0xD5
OpCode   0xD5
Parameter Length   0x0012

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
CSRK	This Connection Signature Resolving Key of the Local Device is used for Data Signing.	16 Bytes

1.31　TCU_LE_SMP_SLV_OOB_KEY_ENTRY_REQ_EVENT

This command is sent by the Slave Device to the application to request to enter the Temporary Key used in the "**Out of Band**" Pairing method. This event is generated as part of pairing process. In response to this event, the application will generate the **"TCU_LE_SMP_SLV_OOB_KEY_ENTRY_WRITE_REQ"** the key write request through which key is input.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes

ServiceID   0xD5
OpCode   0x59
Parameter Length   0x0002

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)

1.32   TCU_LE_SMP_SLV_OOB_KEY_ENTRY_WRITE_REQ

This command contains the Temporary Key entered by the Application for the Slave Device which is used in the **"Out of Band"** Pairing method. This request is generated by the application to Slave Device to input/write the key needed for pairing process.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Status	1 Byte
Key	16 Bytes

ServiceID   0xD5
OpCode   0x1A
Parameter Length   0x0003 or 0x0013

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Status	Result Code: Success Key Entry Failed	0x00 0x01
Key	16 bytes Temporary Key which will contained when Status is success i.e when key is entered through Keyboard Input successfully.	0xXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX

1.33 TCU_LE_SMP_SLV_OOB_KEY_ENTRY_WRITE_RESP

This response is generated by the Slave Device to the Application in response to Out Of Band key write entry request "TCU_LE_SMP_SLV_OOB_KEY_ENTRY_WRITE_REQ".

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Status	1 Byte

ServiceID   0xD5
OpCode   0x9A
Parameter Length   0x0003

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Status	Result Code: - Success - Refer Error Code table	0x00 ---

1.34   TCU_LE_SMP_SLV_STORE_KEY_EVENT

This event is issued by the Slave Device to Application, to request the Application to store/delete the information of the keys exchanged between the Slave Device and the Master Device during pairing. On receiving this event "TCU_LE_SMP_SLV_STORE_KEY_EVENT", based on the event status the application must either store the keys exchanged information in its database onto the Non-Volatile memory or delete the already stored keys exchanged information from the Non-Volatile memory. If the keys exchanged information is stored, on request the same needs to be provided to Slave Device when it connects to a Bonded Master Device.

(Note)

This event is sent to the application under following scenarios:

1. Pairing is completed with a device which has enabled Bonding. After receiving the Pairing Complete Event, the Device sends the event TCU_LE_SMP_SLV_STORE_KEY_EVENT" to indicate to the application that the Key Info of this particular device needs to be stored for future connections.

2.When Pairing Failed Event is received, this event "TCU_LE_SMP_SLV_STORE_KEY_EVENT" is sent to the application to indicate that the Pairing Details associated with this connection handle/BD Address device needs to be deleted.

3. When the Encryption Failure occurs, this event "TCU_LE_SMP_SLV_STORE_KEY_EVENT" is sent to application to indicate that the Pairing Details associated with this connection handle/BD Address device needs to be deleted.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Address Type	1 Byte
BD_Address	6 Bytes
Status	1 Byte

ServiceID   0xD5
OpCode   0xD9
Parameter Length   0x000A

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device keys in database.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Address Type	Indicates the type of the Remote BD Address received Public Address Random Address	 0x00 0x01
BD Address	Indicates the Address of the Remote Device connected.	0xXXXXXXXXXXXX
Status	Indicates whether to store/delete received keys from firmware onto non-volatile memory by application Store Devices Info Delete Device Info	 0x01 0x02

1.35   TCU_LE_SMP_SLV_KEY_REQ_EVENT

This event is sent by the Slave Device to the application to request the application to send the Key Exchanged Information of the Bonded Master Device, stored in the Non-Volatile memory. In response to this event, the application will send all the available keys in its database using the command "TCU_LE_SMP_SLV_KEY_ACCEPT_REQ". If the Remote Master Device is not a Bonded Device, no Keys Exchanged Information will be available. Hence application will not send any keys to the Master Device.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Address Type	1 Byte
BD_Address	6 Bytes

ServiceID   0xD5
OpCode   0xDA
Parameter Length   0x0009

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device keys in database.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Address Type	Indicates the type of the Remote BD Address received Public Address Random Address	 0x00 0x01
BD Address	Indicates the Address of the Remote Device connected.	0xXXXXXXXXXXXX

1.36   TCU_LE_SMP_SLV_KEY_ACCEPT_REQ

This request sends the keys available in the database of the application based on the BD Address and Connection Handle received in the "TCU_LE_SMP_SLV_KEY_REQ_EVENT". If the keys are not available, no keys will be sent and the Status field will be set to "**0x01**".In response to this request, "TCU_LE_SMP_SLV_KEY_ACCEPT_RESP" is received.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Status	1 Byte
KeySetFlag	1 Byte
Remote_EDIV	2 Bytes
Remote_RAND	8 Bytes
Remote_LTK	16 Bytes
Remote_IRK	16 Bytes
Remote_CSRK	16 Bytes
Local_EDIV	2 Bytes
Local_RAND	8 Bytes
Local_LTK	16 Bytes
Local_IRK	16 Bytes
Local_CSRK	16 Bytes
Encryption_Key_Size	1 Byte

ServiceID   0xD5
OpCode   0x1C
Parameter Length: 0x0003 – 0x0078

Parameters:

Parameters	Parameter Description	Value
Conn_Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Status	Indicates whether the Bonding details are available or not. Bonding Details available Bonding Details are not available	 0x00 0x01
KeySetFlag	Bit wise Flag. Indicates the List of Keys present (Note)	0xXX
Remote_EDIV	Encrypted Diversifier Value received from the Remote device.	0xXXXX
Remote_RAND	Random Number received from the Remote device.	0xXXXXXXXXXXXXXXXX
Remote_LTK	Long Tem Key from Remote Device	0xXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXX
Remote_IRK	Identity Resolving Key of the Remote device	0xXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXX
Remote_CSRK	Connection Signature Resolving Key of the Remote device	0xXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXX
Local_EDIV	Encrypted Diversifier Value of the Local Device.	0xXXXX
Local_RAND	Random Number received from the Remote device.	0xXXXXXXXXXXXXXXXX
Local_LTK	Long Tem Key from Remote Device	0xXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXX
Local_IRK	Identity Resolving Key of the Remote device	0xXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXX
Local_CSRK	Connection Signature Resolving Key of the Remote device	0xXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXX
Encryption_Key_Size	Encryption Key Size Value negotiated between Bonded Devices.	7-16

(Note)

The parameter KeySetFlag is used to interpret which all keys are sent by the application. Each bit in the KeySetFlag indicates the presence or absence of the respective keys. The description for the KeySetFlag is depicted in the below table:

KeySetFlag

Size:1 Byte

Value:0xXX

MSB

LSB

Bit 0-Remote LTK,EDIV,Rand
Bit 1-Remote IRK
Bit 2-Remote CSRK
Bit 3-Local LTK,EDIV,Rand
Bit 4-Local IRK
Bit 5-Local CSRK
Bit 6-EncryptKeySize
Bit 7: Reserved

Value="1" indicates LTK,EDIV and Rand of the Remote device is present
Value="0" indicates LTK,EDIV and Rand of the Remote device is not present
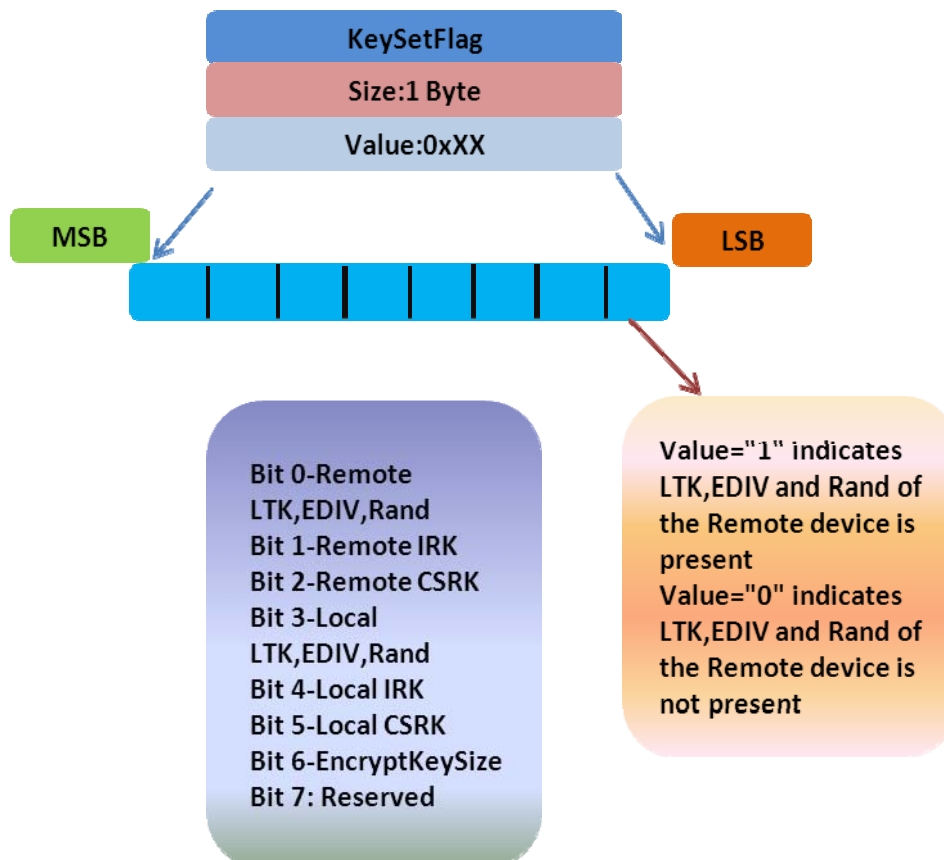
1.37   TCU_LE_SMP_SLV_KEY_ACCEPT_RESP

This response is issued by the Slave Device to the Application in response to Slave Key Accept Request "TCU_LE_SMP_SLV_KEY_ACCEPT_REQ".

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Status	1 Byte

ServiceID   0xD5
OpCode   0x9C
Parameter Length   0x0003

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Status	Result Code: - Success - Refer Error Code table	0x00 ---

1.38 TCU_SMP_LE_SLAVE_BONDING_ENABLED_INFO_REQ

This request is issued by the Slave after the successful connection completion to indicate that the Remote Master Device is a Bonded Device. This information is updated for the GATT Module for further processing of the GATT commands which need to verify that the Remote Device is a Bonded Device. Once the processing of this request is started "**TCU_LE_ACCEPT"** is generated. When this command processing is completed the response **"TCU_SMP_LE_SLAVE_BONDING_ENABLED_INFO_RESP"** is received.

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes

ServiceID 0xD5
OpCode 0x1B
Parameter Length 0x0002

Parameters:

Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)

1.39 TCU_SMP_LE_SLAVE_BONDING_ENABLED_INFO_RESP

This response is generated by the Slave Device to the Slave Application in response to the request "TCU_SMP_LE_SLAVE_BONDING_ENABLED_INFO_REQ".

Command Format:

ServiceID	1 Byte
OpCode	1 Byte
Parameter Length	2 Bytes
Conn_Handle	2 Bytes
Status	1 Byte

ServiceID   0xD5
OpCode   0x9B
Parameter Length   0x0003

Parameters:

| Parameters	Parameter Description	Value
Connection Handle	Connection handle is the index for accessing the remote device.	0x0000 to 0x0EFF (0x0F00 to 0x0FFF Reserved for future use)
Status	Result Code: - Success - Refer Error Code table	0x00 ---

2 Code

2.1   Auth_Req

The Auth_Req field is a bit field that indicates the requested security properties for STK and GAP bonding information
The following figure defines the authentication requirements bit field.

LSB   MSB

Bonding_Falgs (2bits)	MITM (1bit)	Reserved (5bits)

2.2   Init_Key_Dist and Resp_Key_Dist

The format of the Init_Key_Dist field and Resp_Key_Dist field in the Pairing Request and Pairing Response commands for LE is defined in the following figure.

LSB   MSB

EncKey (1bit)	IdKey (1bit)	Sign (1bit)	Reserved (5bits)
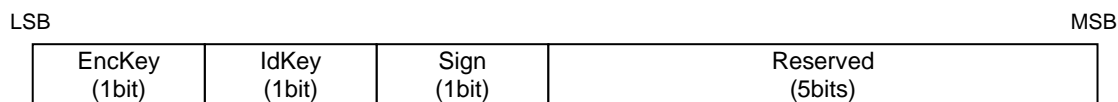
The Key Distribution field has the following flags:
・Enckey is a 1-bit field that is set to one to indicate that the device shall distribute LTK using the Encryption Information command followed by EDIV and Rand using the Master Identification command.
・IdKey is a 1-bit field that is set to one to indicate that the device shall distribute IRK using the identity Information command followed by its public device or static random address using Identity Address Information.
・Sign is a 1-bit field that is set to one to indicate that the device shall distribute CSRK using the Signing Information command.
・Reserved is a 5-bit field that shall be set to zero and ignored on reception.

3 Maximum response time

3.1   Response time from command to response

Command	msec
Under Preparation	

3.2   Response time from command to Event

Command (TCU_LE_SMP_***)	Description	Maximum respond time(s)

Under Preparation

3.3   Recommendation for HOST CPU

When TC35661 does not notify event within above time, TC35661 is under unusual operation.

Then HOST CPU should reset TC35661 with HW-RESET. It is recommended for HOST to consider extra
time from above time.

4   List of error codes

The below table provide information regarding the different Error Code Values used in SMP.

Error	Value
Success	0x00
Passkey Entry Failed	0x01
OOB Not Available	0x02
Authentication Requirements Not Met	0x03
Confirm Value Failed	0x04
Pairing Not Supported	0x05
Encryption Key Size insufficient	0x06
Command Not Supported	0x07
Unspecified Reason	0x08
Repeated Attempts	0x09
Invalid Parameters	0x0A
SMP Time Out	0x0B
SMP timeout has happened previously and no further SMP commands shall be sent over the L2CAP Security Manager Channel till the reconnection happens.	0x0C
Device Not Initialized	0x81
Request in Progress	0x82
Disconnect error	0x84
Invalid parameter Length Error	0x86

Appendex
Appendex A. Definitions and Acronyms

Listed below are the acronyms used in this document:

SL. No	ACRONYM	DEFINITION
1	CID	Channel Identifier
2	EDIV	Encrypted Diversifier
3	CSRK	Connection Signature Resolving Key
4	GAP	Generic Access Profile
5	L2CAP	Logical Link Control and Adaptation Protocol
6	LE	Low Energy
7	LTK	Long Term Key
8	IRK	Identity Resolving Key
9	MAS	Master Device
10	MITM	Man In The Middle
11	OOB	Out Of Band
12	SLV	Slave Device
13	SMP	Security Manager Protocol
14	STK	Short Term Key
15	TBD	To Be Decided
16	TESI	Toshiba Embedded Software India
17	TSBJ	Toshiba Japan

End of document.