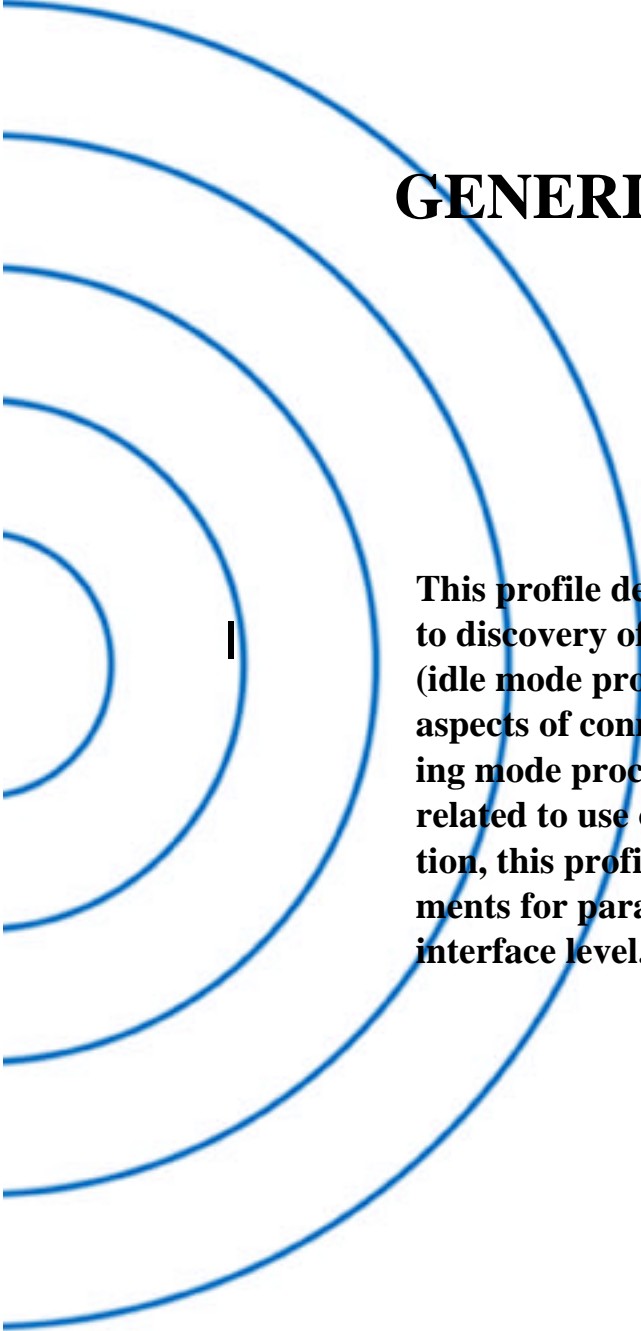


Part K:1

GENERIC ACCESS PROFILE



This profile defines the generic procedures related to discovery of Bluetooth devices (idle mode procedures) and link management aspects of connecting to Bluetooth devices (connecting mode procedures). It also defines procedures related to use of different security levels. In addition, this profile includes common format requirements for parameters accessible on the user interface level.



CONTENTS

1	Introduction.....	20
1.1	Scope	20
1.2	Symbols and conventions	20
1.2.1	Requirement status symbols.....	20
1.2.2	Signalling diagram conventions	21
1.2.3	Notation for timers and counters	21
2	Profile overview	22
2.1	Profile stack	22
2.2	Configurations and roles	22
2.3	User requirements and scenarios	23
2.4	Profile fundamentals.....	23
2.5	Conformance	24
3	User interface aspects	25
3.1	The user interface level	25
3.2	Representation of Bluetooth parameters	25
3.2.1	Bluetooth device address (BD_ADDR)	25
3.2.1.1	Definition	25
3.2.1.2	Term on user interface level.....	25
3.2.1.3	Representation	25
3.2.2	Bluetooth device name (the user-friendly name)	25
3.2.2.1	Definition	25
3.2.2.2	Term on user interface level.....	26
3.2.2.3	Representation	26
3.2.3	Bluetooth passkey (Bluetooth PIN)	26
3.2.3.1	Definition	26
3.2.3.2	Term on Terms at user interface level.....	26
3.2.3.3	Representation	26
3.2.4	Class of Device	27
3.2.4.1	Definition	27
3.2.4.2	Term on user interface level.....	27
3.2.4.3	Representation	27
3.3	Pairing	28



4	Modes	29
4.1	Discoverability modes	29
4.1.1	Non-discoverable mode	30
4.1.1.1	Definition	30
4.1.1.2	Term on UI-level	30
4.1.2	Limited discoverable mode	30
4.1.2.1	Definition	30
4.1.2.2	Conditions	31
4.1.2.3	Term on UI-level	31
4.1.3	General discoverable mode	31
4.1.3.1	Definition	31
4.1.3.2	Conditions	31
4.1.3.3	Term on UI-level	31
4.2	Connectability modes	31
4.2.1	Non-connectable mode	31
4.2.1.1	Definition	31
4.2.1.2	Term on UI-level	32
4.2.2	Connectable mode	32
4.2.2.1	Definition	32
4.2.2.2	Term on UI-level	32
4.3	Pairing modes	32
4.3.1	Non-pairable mode	32
4.3.1.1	Definition	32
4.3.1.2	Term on UI-level	32
4.3.2	Pairable mode	32
4.3.2.1	Definition	32
4.3.2.2	Term on UI-level	32
5	Security aspects	33
5.1	Authentication	33
5.1.1	Purpose	33
5.1.2	Term on UI level	33
5.1.3	Procedure	34
5.1.4	Conditions	34
5.2	Security modes	34
5.2.1	Security mode 1 (non-secure)	36
5.2.2	Security mode 2 (service level enforced security)	36
5.2.3	Security modes 3 (link level enforced security)	36



6	Idle mode procedures	37
6.1	General inquiry	37
6.1.1	Purpose	37
6.1.2	Term on UI level	37
6.1.3	Description	38
6.1.4	Conditions	38
6.2	Limited inquiry	38
6.2.1	Purpose	38
6.2.2	Term on UI level	39
6.2.3	Description	39
6.2.4	Conditions	39
6.3	Name discovery	40
6.3.1	Purpose	40
6.3.2	Term on UI level	40
6.3.3	Description	40
	6.3.3.1 Name request	40
	6.3.3.2 Name discovery	40
6.3.4	Conditions	41
6.4	Device discovery	41
6.4.1	Purpose	41
6.4.2	Term on UI level	41
6.4.3	Description	42
6.4.4	Conditions	42
6.5	Bonding	42
6.5.1	Purpose	42
6.5.2	Term on UI level	42
6.5.3	Description	43
	6.5.3.1 General bonding	43
	6.5.3.2 Dedicated bonding	44
6.5.4	Conditions	44



7	Establishment procedures	45
7.1	Link establishment	45
7.1.1	Purpose	45
7.1.2	Term on UI level	45
7.1.3	Description	46
	7.1.3.1 B in security mode 1 or 2	46
	7.1.3.2 B in security mode 3	47
7.1.4	Conditions	47
7.2	Channel establishment	48
7.2.1	Purpose	48
7.2.2	Term on UI level	48
7.2.3	Description	48
	7.2.3.1 B in security mode 2	49
	7.2.3.2 B in security mode 1 or 3	49
7.2.4	Conditions	49
7.3	Connection establishment	50
7.3.1	Purpose	50
7.3.2	Term on UI level	50
7.3.3	Description	50
	7.3.3.1 B in security mode 2	50
	7.3.3.2 B in security mode 1 or 3	51
7.3.4	Conditions	51
7.4	Establishment of additional connection	51
8	Definitions	52
8.1	General General definitions	52
8.2	Connection related Connection-related definitions	52
8.3	Device related Device-related definitions	53
8.4	Procedure related Procedure-related definitions	54
8.5	Security related Security-related definitions	54
9	Annex A (Normative): Timers and constants	56
10	Annex B (Informative): Information flows of related procedures	57
10.1	Imp-authentication	57
10.2	Imp-pairing	57 58
10.3	Service discovery	58
11	References	60



FOREWORD

- Interoperability between devices from different manufacturers is provided for a specific service and use **case case**, if the devices conform to a Bluetooth **SIG SIG**-defined profile specification. A profile defines a selection of messages and procedures (generally termed *capabilities*) from the Bluetooth SIG specifications and gives an unambiguous description of the air interface for specified service(s) and use case(s).
- All defined features are **process process**-mandatory. This means **that that**, if a feature is used, it is used in a specified manner. Whether the provision of a feature is mandatory or optional is stated separately for both sides of the Bluetooth air interface.

1 INTRODUCTION

1.1 SCOPE

The purpose of the Generic Access Profile is:

To introduce definitions, recommendations and common requirements related to modes and access procedures that are to be used by transport and application profiles.

To describe how devices are to behave in standby and connecting states in order to guarantee that links and channels always can be established between Bluetooth **devices**, and that multi-profile operation is possible. Special focus is put on discovery, link establishment and security procedures.

To state requirements on user interface aspects, mainly coding schemes and names of procedures and parameters, that are needed to guarantee a satisfactory user experience.

1.2 SYMBOLS AND CONVENTIONS

1.2.1 Requirement status symbols

In this document (especially in the profile requirements tables), the following symbols are used:

"M" for mandatory to support (used for capabilities that shall be used in the profile);

"O" for optional to support (used for capabilities that can be used in the profile);

"C" for conditional support (used for capabilities that shall be used in case a certain other capability is supported);

"X" for excluded (used for capabilities that may be supported by the unit but shall never be used in the profile);

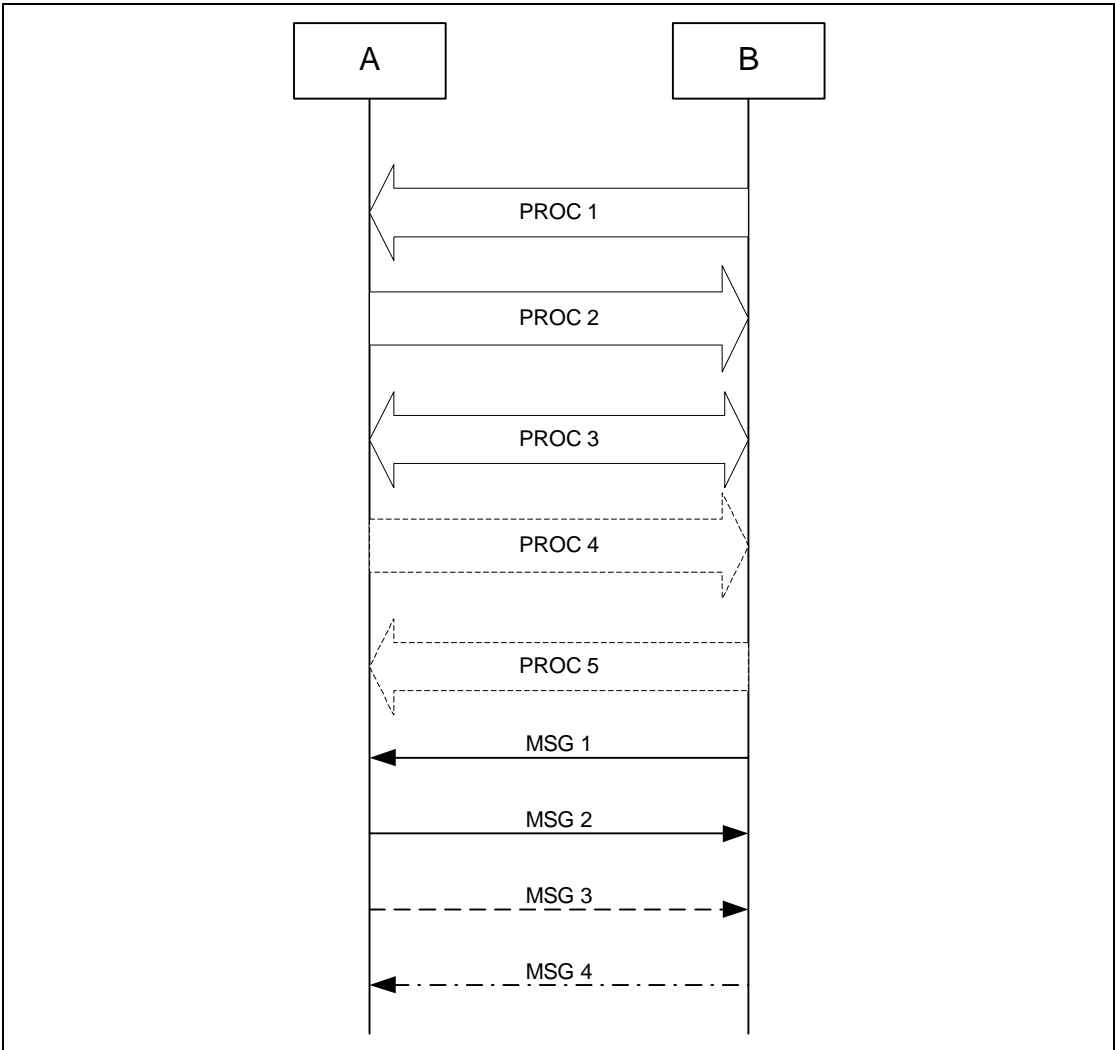
"N/A" for not applicable (in the given context it is impossible to use this capability).

Some excluded capabilities are capabilities that, according to the relevant Bluetooth specification, are mandatory. These are features that may degrade operation of devices following this profile. Therefore, these features shall never be activated while a unit is operating as a unit within this profile.

In this **specification**, the word *shall* is used for mandatory requirements, the word *should* is used to express recommendations and the word *may* is used for options.

1.2.2 Signalling diagram conventions

The following arrows are used in diagrams describing procedures :



A		B
	PROC1	
	PROC2	
	PROC3	
	(PROC4)	
	(PROC5)	



	MSG1	
	MSG2	
	(MSG3)	
	(MSG4)	

Figure 1.1: Arrows used in signalling diagrams

In the table above, the following cases are shown: PROC1 is a **subprocedure sub-procedure** initiated by B. PROC2 is a **subprocedure sub-procedure** initiated by A. PROC3 is a **subprocedure sub-procedure** where the initiating side is undefined (may be both A and or B). Dashed arrows denote optional steps. PROC4 indicates an optional **subprocedure sub-procedure** initiated by A, and PROC5 indicates an optional **subprocedure sub-procedure** initiated by B.

MSG1 is a message sent from B to A. MSG2 is a message sent from A to B. MSG3 indicates an optional message from A to B, and MSG4 indicates a conditional message from B to A.

1.2.3 Notation for timers and counters

Timers are introduced specific to this profile. To distinguish them from timers used in the Bluetooth protocol specifications and other profiles, these timers are named in the following format: **"T_{GAP}(nnn)"**.

2 PROFILE OVERVIEW

2.1 PROFILE STACK

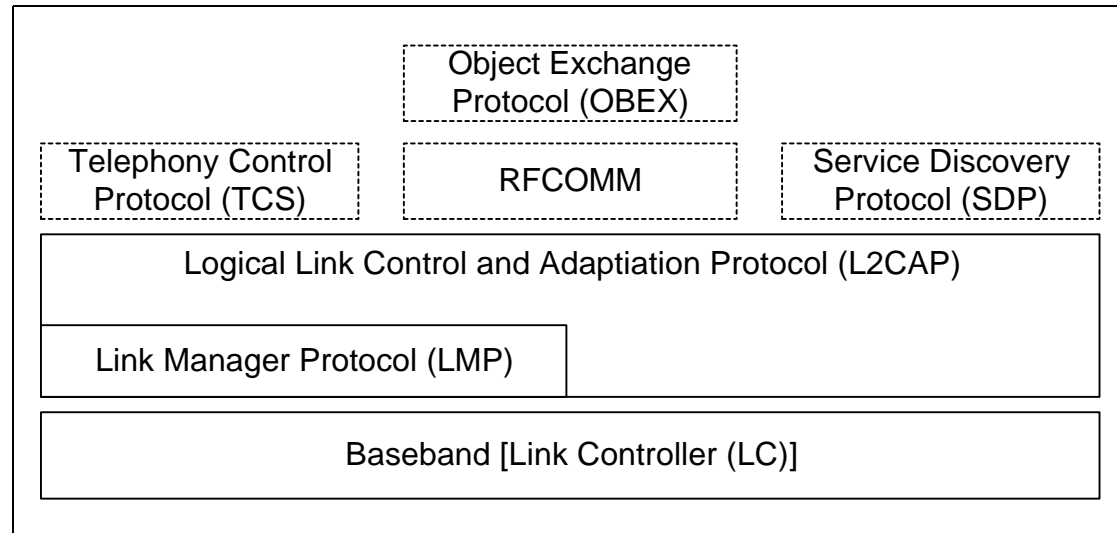


Figure 2.1: Profile stack covered by this profile.

The main purpose of this profile is to describe the use of the lower layers of the Bluetooth protocol stack (LC and LMP). To describe security related alternatives, also higher layers (L2CAP, RFCOMM and OBEX) are included.

2.2 CONFIGURATIONS AND ROLES

For the descriptions in this profile of the roles that the two devices involved in a Bluetooth communication can take, the generic notation of the A-party (the *paging device* in case of link **establishment**, or *initiator* in case of another procedure on an established link) and the B-party (*paged device* or *acceptor*) is used. The A-party is the one **that**, for a given **procedure**, initiates the establishment of the physical link or initiates a transaction on an existing link.

This profile handles the procedures between two devices related to discovery and connecting (link and connection establishment) for the case where none of the two devices has any link established as well as the case where (at least) one device has a link established (possibly to a third device) before starting the described procedure.

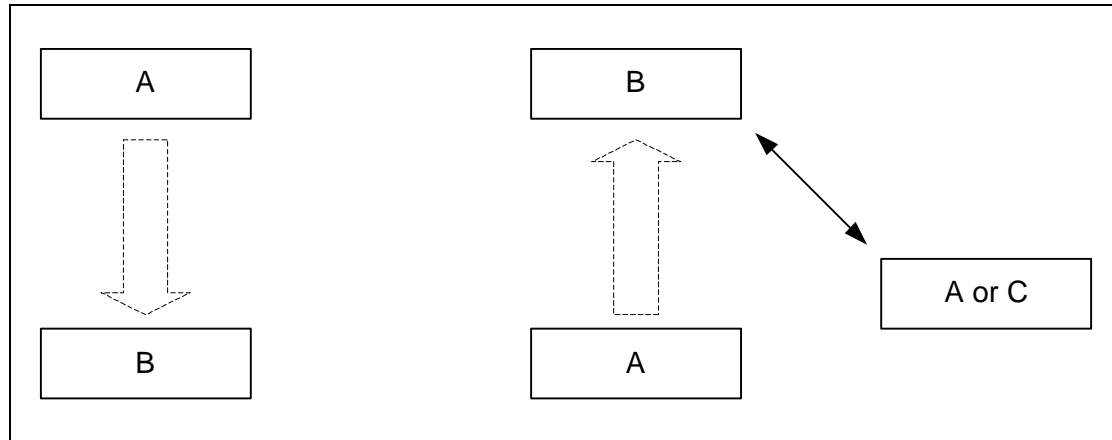


Figure 2.2: This profile covers procedures *initiated* by one device (A) towards another device (B) that may or may not have an existing Bluetooth link active.

The initiator and the acceptor generally operate the generic procedures according to this profile or another profile referring to this profile. If the acceptor operates according to several profiles simultaneously, this profile describes generic mechanisms for how to handle this.

2.3 USER REQUIREMENTS AND SCENARIOS

The Bluetooth user should in principle be able to connect a Bluetooth device to any other Bluetooth device. Even if the two connected devices don't share any common application, it should be possible for the user to find this out using basic Bluetooth capabilities. When the two devices do share the same application but are from different manufacturers, the ability to connect them should not be blocked just because manufacturers choose to call basic Bluetooth capabilities by different names on the user interface level or implement basic procedures to be executed in different orders.

2.4 PROFILE FUNDAMENTALS

This profile states the requirements on names, values and coding schemes used for names of parameters and procedures experienced on the user interface level.

This profile defines modes of operation that are not *service or profile specific* *service- or profile-specific*, but that are generic and can be used by profiles referring to this *profile*, and by devices implementing multiple profiles.

This profile defines the general procedures that can be used for discovering identities, names and basic capabilities of other Bluetooth devices that are in a mode where they can be discoverable. Only procedures where no channel or connection establishment is used are specified.

This profile defines the general procedure for how to create bonds (i.e. dedicated exchange of link keys) between Bluetooth devices.



This profile describes the general procedures that can be used for establishing connections to other Bluetooth devices that are in mode that allows them to accept connections and service requests.

2.5 CONFORMANCE

Bluetooth devices that do not conform to any other Bluetooth profile shall conform to this profile to ensure basic interoperability and co-existence.

Bluetooth devices that conform to another Bluetooth profile may use adaptations of the generic procedures as specified by that other profile. They shall, however, be compatible with devices compliant to this profile at least on the level of the supported generic procedures.

If conformance to this profile is claimed, all capabilities indicated mandatory for this profile shall be supported in the specified manner (process process-mandatory). This also applies for all optional and conditional capabilities for which support is indicated. All mandatory capabilities, and optional and conditional capabilities for which support is indicated, are subject to verification as part of the Bluetooth certification programmeprogram.



3 USER INTERFACE ASPECTS

3.1 THE USER INTERFACE LEVEL

In the context of this specification, the user interface level refers to places (such as displays, **dialogue** **dialog** boxes, manuals, packaging, **advertising** **advertising**, etc.) where users of Bluetooth devices encounter names, values and numerical representation of Bluetooth terminology and parameters.

This profile specifies the generic terms that should be used on the user interface level. These terms should be translated into languages supported by the Bluetooth device according to tables provided by the Bluetooth SIG.

3.2 REPRESENTATION OF BLUETOOTH PARAMETERS

3.2.1 Bluetooth device address (BD_ADDR)

3.2.1.1 Definition

BD_ADDR is the unique address of a Bluetooth device as defined in [1]. It is received from a remote device during the device discovery procedure.

3.2.1.2 Term on user interface level

When the Bluetooth address is referred to on UI level, the term “Bluetooth Device Address” should be used.

3.2.1.3 Representation

On BB level the BD_ADDR is represented as 48 bits [1].

On the UI level the Bluetooth address shall be represented as 12 hexadecimal characters, possibly divided into sub-parts separated by “:” or “-”. (E.g., “000C3E3A4B69” or “00:0C:3E:3A:4B:69”). At UI level, any number shall have the MSB -> LSB (from left to right) “natural” ordering (e.g., the number “16” shall be shown as “0x10”).

3.2.2 Bluetooth device name (the user-friendly name)

3.2.2.1 Definition

The Bluetooth device name is the user-friendly name that a Bluetooth device presents itself with. It is a character string returned in LMP_name_res as response to a LMP_name_req.



3.2.2.2 Term on user interface level

When the Bluetooth device name is referred to on UI level, the term “Bluetooth Device Name” should be used.

3.2.2.3 Representation

The Bluetooth device name can be up to 248 bytes maximum according to [2]. It shall be coded according to Unicode UTF-8 (i.e. name entered on UI level may be down to 82 characters if UCS-2 is used).

A device can not expect that a general remote device is able to handle more than the first 40 characters of the Bluetooth device name. If a remote device has limited display capabilities, it may use only the first 20 characters.

3.2.3 Bluetooth passkey (Bluetooth PIN)

3.2.3.1 Definition

The Bluetooth PIN is used to authenticate two Bluetooth devices (that have not previously exchanged link keys) to each other and create a trusted relationship between them. The PIN is used in the pairing procedure (see Section 10.2) to generate the initial link key that is used for further authentication.

The PIN may be entered on UI level but may also be stored in the device, ; e.g. in the case of a device without sufficient MMI for entering and displaying digits.

3.2.3.2 Term on Terms at user interface level

When the Bluetooth PIN is referred to on UI level, the term “Bluetooth Passkey” should be used.

3.2.3.3 Representation

The Bluetooth PIN has different representations on different level. PIN_{BB} is used on baseband level, and PIN_{UI} is used on user interface level.

PIN_{BB} is the PIN used by [1] for calculating the initialisation initialization key during the pairing procedure. PIN_{UI} is the character representation of the PIN that is entered on UI level. The transformation between PIN_{BB} and PIN_{UI} shall be according to Unicode UTF-8.

According to [1], PIN_{BB} can be 128 bits (16 bytes). When PIN is entered on UI level (PIN_{UI}), it is to be coded into PIN_{BB} according to Unicode UTF-8 (i.e. if a device sup-



ports entry of characters outside the Unicode range 0x00 - 0x7F, the maximum number of characters in the PIN_{UI} may be less than 16).

Examples:

User User -entered code	Corresponding $PIN_{BB}[0..length-1]$ (value as a sequence of octets in hexadecimal notation)
"0123"	length = 4, value = 0x30 0x31 0x32 0x33
"Ärlich"	length = 7, value = 0xC3 0x84 0x72 0x6C 0x69 0x63 0x68

All Bluetooth devices that support the bonding procedure and support PIN handling on UI level shall support UI level handling of PINs consisting of decimal digits. In addition, devices may support UI level handling of PINs consisting of general characters.

When defining the value of its PIN, a device that is expected to pair with a remote device that has restricted UI capabilities shall use a PIN that can be entered on UI level as decimal digits.

If a device has a fixed PIN (i.e. PIN is stored in the device and cannot be entered on UI level during pairing), the PIN shall be defined using decimal digits. A device that is expected to pair with a remote device that has restricted UI capabilities should ensure that the PIN can be entered on UI level as decimal digits.

3.2.4 Class of Device

3.2.4.1 Definition

Class of device is a parameter received during the device discovery **procedure**, indicating the type of device and which types of service that are supported.

3.2.4.2 Term on user interface level

The information within the Class of Device parameter should be referred to as “Bluetooth Device Class” (i.e. the major and minor device class fields) and “Bluetooth Service Type” (i.e. the service class field). The terms for the defined Bluetooth Device Types and Bluetooth Service Types are defined in [11].

When using a mix of information found in the Bluetooth Device Class and the Bluetooth Service Type, the term “Bluetooth Device Type” should be used.



3.2.4.3 Representation

The Class of device is a bit field and is defined in [11]. The UI-level representation of the information in the Class of device is implementation specific.

3.3 PAIRING

Two procedures are defined that make use of the pairing procedure defined on LMP level (lmpLMP-pairing, see Section 10.2). Either the user initiates the bonding procedure and enters the passkey with the explicit purpose of creating a bond (and maybe also a trusted secure relationship) between two Bluetooth devices, or the user is requested to enter the passkey during the establishment procedure since the devices did not share a common link key beforehand. In the first case, the user is said to perform “bonding (with entering of passkey)” and in the second case the user is said to “authenticate using the passkey”.

4 MODES

	Procedure	Ref.	Support
1	Discoverability modes	4.1	
	Non-discoverable mode		C1
	Limited discoverable mode		C2
	General discoverable mode		C2
2	Connectability modes	4.1.3.3	
	Non-connectable mode		O
	Connectable mode		M
3	Pairing modes	4.2.2.2	
	Non-pairable mode		O
	Pairable mode		C3
C1: If limited discoverable mode is supported, non-discoverable mode is mandatory, otherwise optional.			
C2: A Bluetooth device shall support at least one discoverable mode (limited or/and general).			
C3: If the bonding procedure is supported, support for pairable mode is mandatory, otherwise optional.			

Table 4.1: Conformance requirements related to modes defined in this section

4.1 DISCOVERABILITY MODES

With respect to inquiry, a Bluetooth device shall be either in non-discoverable mode or in a discoverable mode. (The device shall be in one, and only one, discoverability mode at a time.) The two discoverable modes defined here are called limited discoverable mode and general discoverable mode. Inquiry is defined in [1].

When a Bluetooth device is in non-discoverable mode it does not respond to inquiry.

A Bluetooth device is said to be made discoverable, or set into a discoverable mode, when it is in limited discoverable mode or in general discoverable mode. Even when a Bluetooth device is made discoverable it may be unable to respond to inquiry due to other baseband activity [1]. A Bluetooth device that does not respond to inquiry for any of these two reasons is called a silent device.

After being made discoverable, the Bluetooth device shall be discoverable for at least $T_{\text{GAP}}(103)$.



4.1.1 Non-discoverable mode

4.1.1.1 Definition

- | When a Bluetooth device is in non-discoverable **mode mode**, it shall never enter the INQUIRY_RESPONSE state.

4.1.1.2 Term on UI-level

- | Bluetooth device is “non-discoverable” or in “non-discoverable mode”.

4.1.2 Limited discoverable mode

4.1.2.1 Definition

The limited discoverable mode should be used by devices that need to be discoverable only for a limited period of time, during temporary conditions or for a specific event. The purpose is to respond to a device that makes a limited inquiry (inquiry using the LIAC).

A Bluetooth device should not be in limited discoverable mode for more than $T_{GAP}(104)$. The scanning for the limited inquiry access code can be done either in parallel or in sequence with the scanning of the general inquiry access code. When in limited discoverable mode, one of the following options shall be used.

4.1.2.1.1 Parallel scanning

When a Bluetooth device is in limited discoverable mode, it shall enter the INQUIRY_SCAN state at least once in $T_{GAP}(102)$ and scan for the GIAC and the LIAC for at least $T_{GAP}(101)$.

4.1.2.1.2 Sequential scanning

When a Bluetooth device is in limited discoverable mode, it shall enter the INQUIRY_SCAN state at least once in $T_{GAP}(102)$ and scan for the GIAC for at least $T_{GAP}(101)$ and enter the INQUIRY_SCAN state more often than once in $T_{GAP}(102)$ and scan for the LIAC for at least $T_{GAP}(101)$.

If an inquiry message is received when in limited discoverable mode, the entry into the INQUIRY_RESPONSE state takes precedence over the next entries into INQUIRY_SCAN state until the inquiry response is completed.



4.1.2.2 Conditions

When a device is in limited discoverable mode it shall set bit no 13 in the Major Service Class part of the Class of Device/Service field [11].

4.1.2.3 Term on UI-level

Bluetooth device is “discoverable” or in “discoverable mode”.

4.1.3 General discoverable mode

4.1.3.1 Definition

The general discoverable mode shall be used by devices that need to be discoverable continuously or for no specific condition. The purpose is to respond to a device that makes a general inquiry (inquiry using the GIAC).

4.1.3.2 Conditions

When a Bluetooth device is in general discoverable mode, it shall enter the INQUIRY_SCAN state more often than once in $T_{GAP}(102)$ and scan for the GIAC for at least $T_{GAP}(101)$.

A device in general discoverable mode shall not respond to a LIAC inquiry.

4.1.3.3 Term on UI-level

Bluetooth device is “discoverable” or in “discoverable mode”.

4.2 CONNECTABILITY MODES

With respect to paging, a Bluetooth device shall be either in non-connectable mode or in connectable mode. Paging is defined in [1].

When a Bluetooth device is in non-connectable mode it does not respond to paging.
When a Bluetooth device is in connectable mode it responds to paging.

4.2.1 Non-connectable mode

4.2.1.1 Definition

When a Bluetooth device is in non-connectable mode it shall never enter the PAGE_SCAN state.



4.2.1.2 Term on UI-level

- | Bluetooth device is “non-connectable” or in “non-connectable mode”.

4.2.2 Connectable mode

4.2.2.1 Definition

When a Bluetooth device is in connectable mode it shall periodically enter the PAGE_SCAN state.

4.2.2.2 Term on UI-level

- | Bluetooth device is “connectable” or in “connectable mode”.

4.3 PAIRING MODES

- | With respect to pairing, a Bluetooth device shall be either in non-pairable mode or in pairable mode. In pairable mode the Bluetooth device accepts **paring**, **paring** – i.e. creation of **bonds**, **bonds** – initiated by the remote **device device**, and in non-pairable mode it does not. Pairing is defined in [1] and [2].

4.3.1 Non-pairable mode

4.3.1.1 Definition

When a Bluetooth device is in non-pairable mode it shall respond to a received LMP_in_rand with LMP_not_accepted with the reason *pairing not allowed*.

4.3.1.2 Term on UI-level

- | Bluetooth device is “non-bondable” or in “non-bondable mode” or “does not accept bonding”.

4.3.2 Pairable mode

4.3.2.1 Definition

When a Bluetooth device is in pairable mode it shall respond to a received LMP_in_rand with LMP_accepted (or with LMP_in_rand if it has a fixed PIN).

4.3.2.2 Term on UI-level

- | Bluetooth device is “bondable” or in “bondable mode” or “accepts bonding”.



5 SECURITY ASPECTS

	Procedure	Ref.	Support
1	Authentication	5.1	C1
2	Security modes	5.2	
	Security mode 1		O
	Security mode 2		C2
	Security mode 3		C2
C1: If security mode 1 is the only security mode that is supported, support for authentication is optional, otherwise mandatory. (Note: support for lmpLMP -authentication and lmpLMP -pairing is mandatory according [2] independent of which security mode that is used.)			
C2: If security mode 1 is not the only security mode that is supported, then support for at least one of security mode 2 or security mode 3 is mandatory.			

Table 5.1: Conformance requirements related to the generic authentication procedure and the security modes defined in this section

5.1 AUTHENTICATION

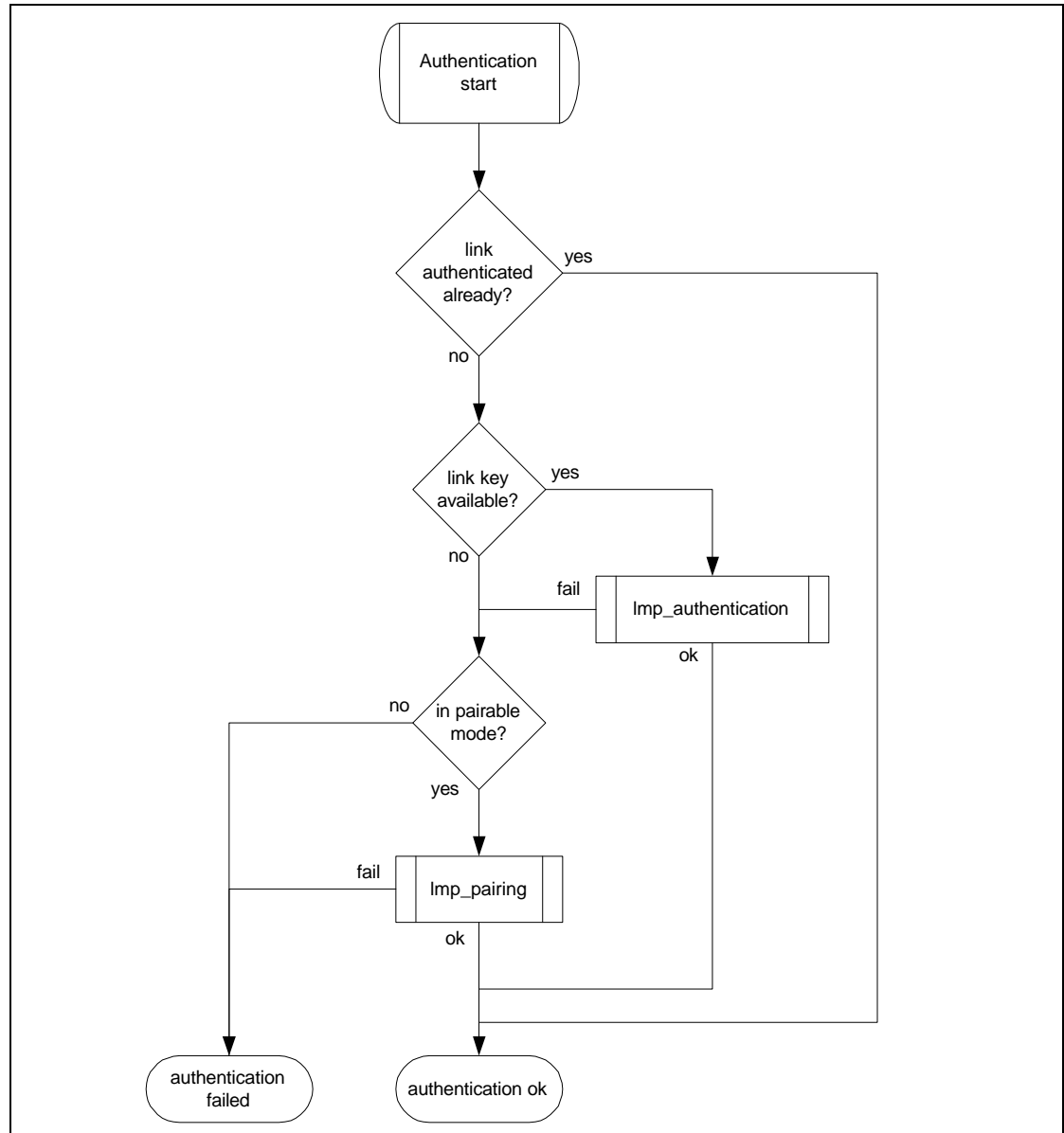
5.1.1 Purpose

The generic authentication procedure describes how the **lmpLMP**-authentication and **lmpLMP**-pairing procedures are used when authentication is initiated by one Bluetooth device towards **another another**, depending on if a link key **exist exists** or not and if pairing is allowed or not.

5.1.2 Term on UI level

“Bluetooth authentication”.

5.1.3 Procedure

I

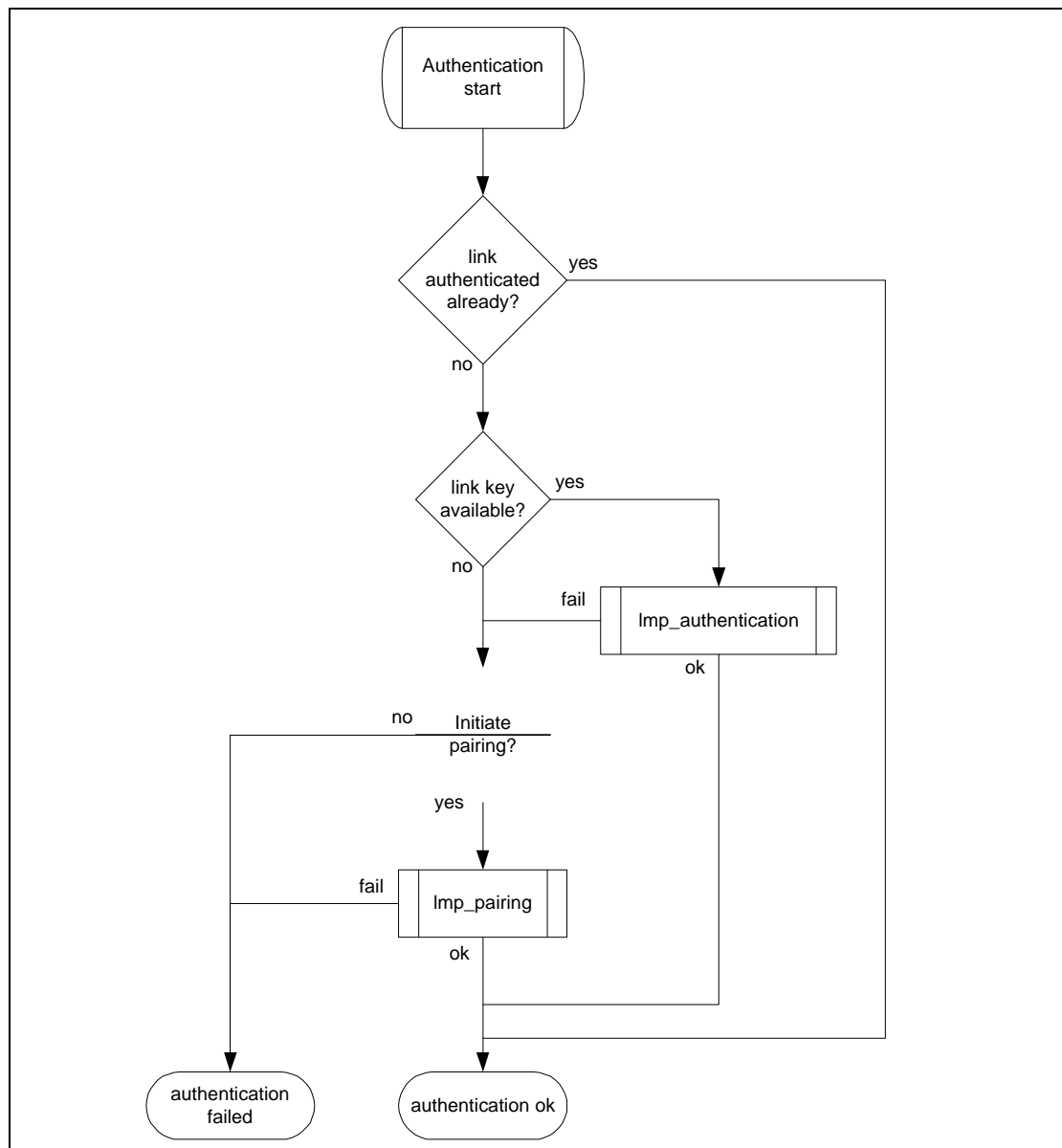


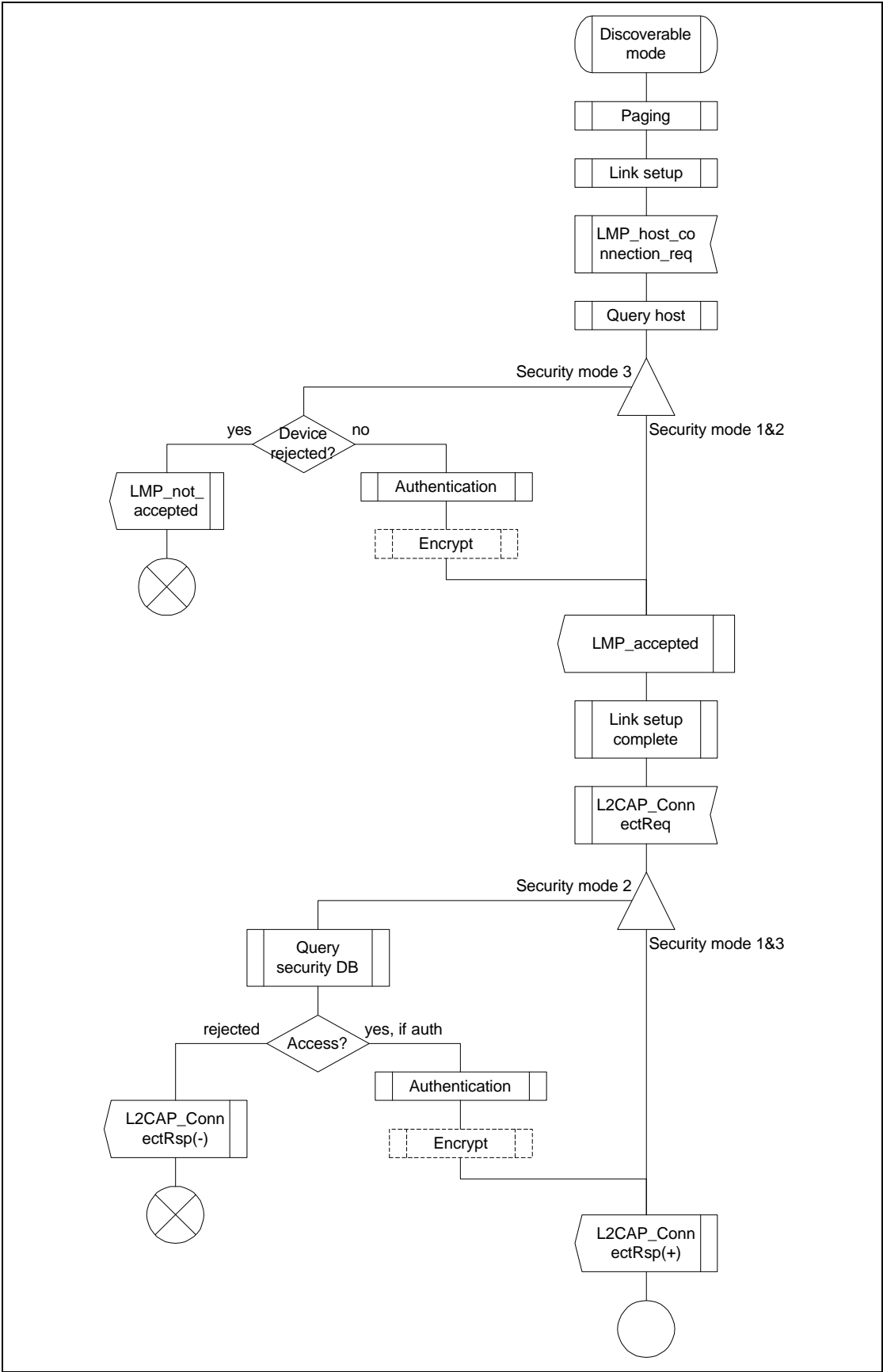
Figure 5.1: Definition of the generic authentication procedure.

5.1.4 Conditions

The device that initiates authentication has to be in security mode 2 or in security mode 3.

5.2 SECURITY MODES

The following flow chart describes where in the channel establishment procedures initiation of authentication takes place, depending on which security mode the Bluetooth device is in.



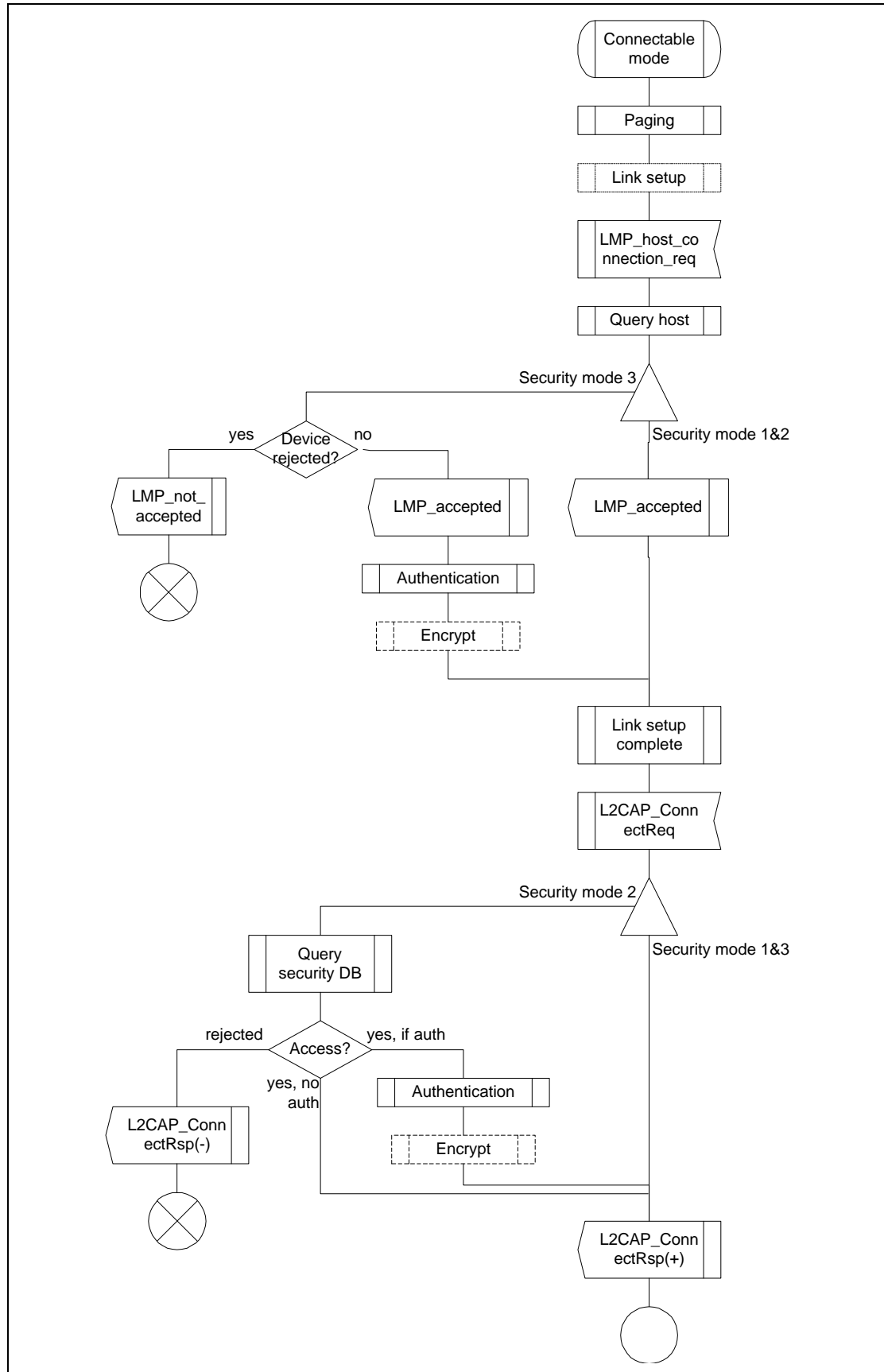


Figure 5.2: Illustration of channel establishment using different security modes.



When authentication is initiated towards a Bluetooth device, it shall act according to [2] and the current pairing **mode mode**, independent of which security mode it is in.

5.2.1 Security mode 1 (non-secure)

When a Bluetooth device is in security mode 1 it shall never initiate any security procedure (i.e., it shall never send LMP_au_rand, LMP_in_rand or LMP_encryption_mode_req).

5.2.2 Security mode 2 (service level enforced security)

When a Bluetooth device is in security mode 2 it shall not initiate any security procedure before a channel establishment request (L2CAP_ConnectReq) has been received or a channel establishment procedure has been initiated by itself. (The **behaviour behavior** of a device in security mode 2 is further described in [10].) Whether a security procedure is initiated or not depends on the security requirements of the requested channel or service.

A Bluetooth device in security mode 2 should classify the security requirements of its services using at least the following attributes:

- **Authorisation Authorization** required;
- Authentication required;
- Encryption required.

Note: Security mode 1 can be considered (at least from a remote device point of view) as a special case of security mode 2 where no service has registered any security requirements.

5.2.3 Security modes 3 (link level enforced security)

When a Bluetooth device is in security mode 3 it shall initiate security procedures before it sends LMP_link_setup_complete. (The **behaviour behavior** of a device in security mode 3 is as described in [2].)

A Bluetooth device in security mode 3 may reject the host connection request (respond with LMP_not_accepted to the LMP_host_connection_req) based on settings in the host (e.g. only communication with pre-paired devices allowed).



6 IDLE MODE PROCEDURES

The inquiry and discovery procedures described here are applicable only to the device that initiates them (A). The requirements on the behaviour behavior of B is according to the modes specified in Section 4 and to [2].

	Procedure	Ref.	Support
1	General inquiry	6.1	C1
2	Limited inquiry	6.2	C1
3	Name discovery	6.3	O
4	Device discovery	6.4	O
5	Bonding	6.5	O
C1: If initiation of bonding is supported, support for at least one inquiry procedure is mandatory, otherwise optional. (Note: support for impLMP -pairing is mandatory [2].)			

6.1 GENERAL INQUIRY

6.1.1 Purpose

The purpose of the general inquiry procedure is to provide the initiator with the Bluetooth device address, clock, Class of Device and used page scan mode of general discoverable devices (i.e., . devices that are in range w.r.t. with regard to the initiator and are set to scan for inquiry messages with the General Inquiry Access Code). Also devices in limited discoverable mode will be discovered using general inquiry.

The general inquiry should be used by devices that need to discover devices that are made discoverable continuously or for no specific condition.

6.1.2 Term on UI level

“Bluetooth Device Inquiry”.

6.1.3 Description

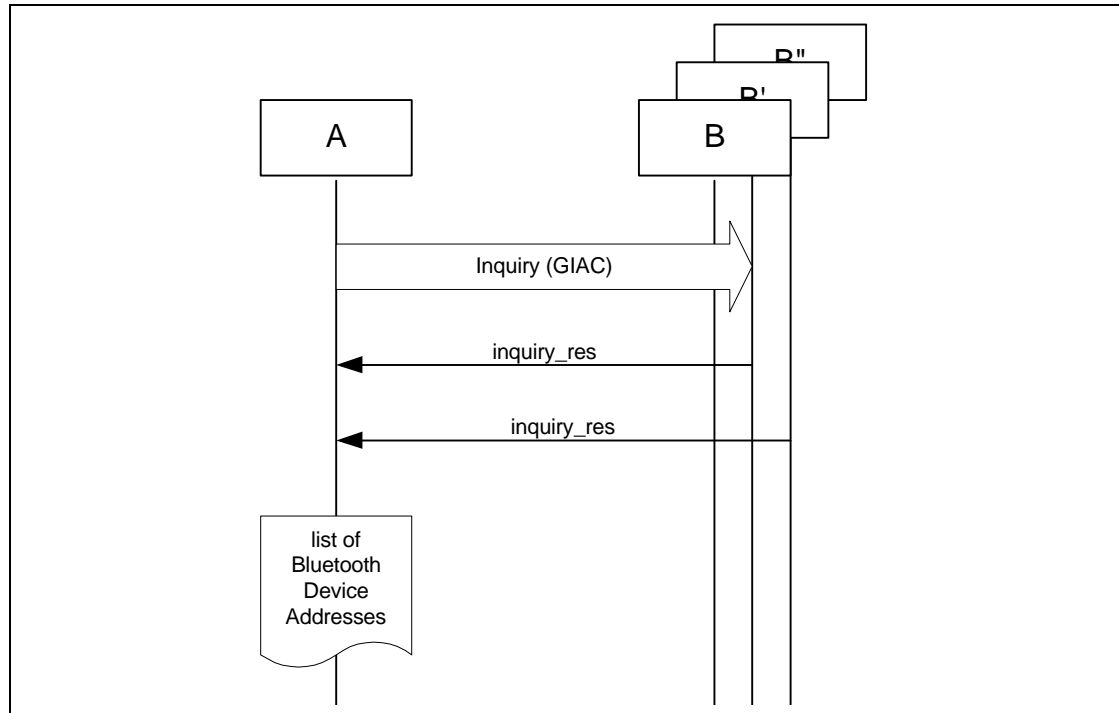


Figure 6.1: General inquiry, where *B* is a device in non-discoverable mode, *B'* is a device in limited discoverable mode and *B''* is a device in general discoverable mode. (Note that all discoverable devices are discovered using general *inquiry inquiry*, independent of which discoverable mode they are in.)

6.1.4 Conditions

When general inquiry is initiated by a Bluetooth device, it shall be in the INQUIRY state for at least $T_{GAP}(100)$ and perform inquiry using the GIAC.

- In order to receive inquiry response, the remote devices in range *has have* to be made discoverable (limited or general).

6.2 LIMITED INQUIRY

6.2.1 Purpose

The purpose of the limited inquiry procedure is to provide the initiator with the Bluetooth device address, clock, Class of Device and used page scan mode of limited discoverable devices. The latter devices are devices that are in range *w.r.t. the initiator with regard to the initiator*, and may be set to scan for inquiry messages with the Limited Inquiry Access *Code Code*, in addition to scanning for inquiry messages with the General Inquiry Access Code.

The limited inquiry should be used by devices that need to discover devices that are made discoverable only for a limited period of time, during temporary conditions or for a specific event. Since it is not guaranteed that the discoverable device scans for the LIAC, the initiating device may choose any inquiry

procedure (general or limited). Even if the remote device that is to be discovered is expected to be made limited discoverable (as e.g. when a dedicated bonding is to be performed), the limited inquiry should be done in sequence with a general inquiry in such a way that both inquiries are completed within the time the remote device is limited discoverable, i.e. at least $T_{\text{GAP}}(103)$.

6.2.2 Term on UI level

“Bluetooth Device Inquiry”.

6.2.3 Description

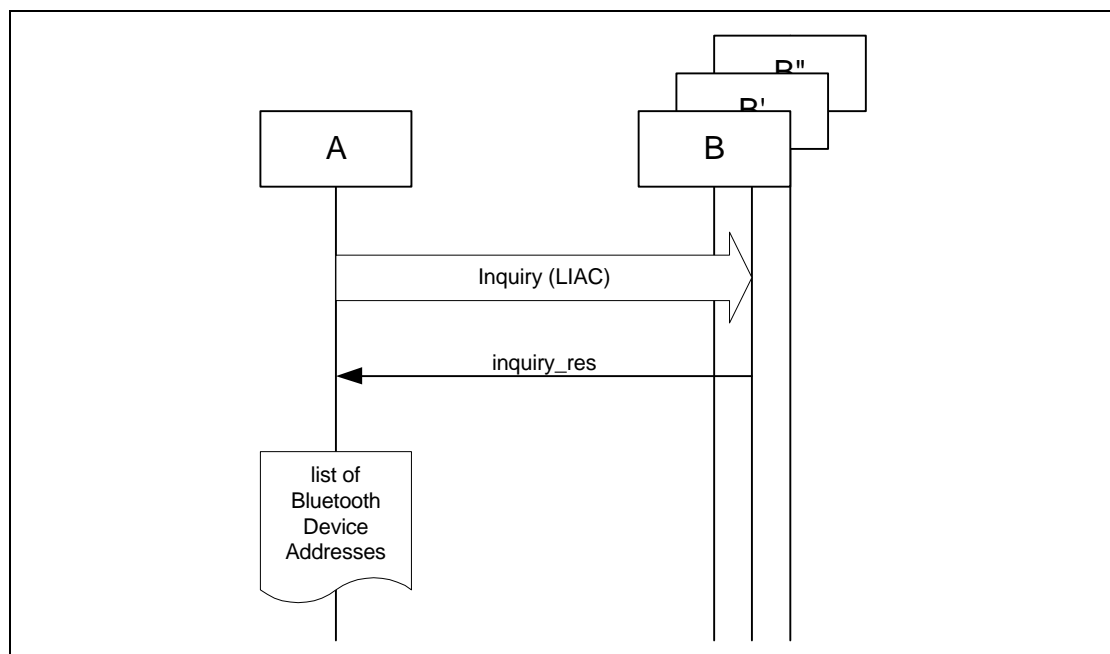


Figure 6.2: Limited inquiry where B is a device in non-discoverable mode, B' is a device in limited discoverable mode and B'' is a device in general discoverable mode. (Note that only limited discoverable devices can be discovered using limited inquiry.)

6.2.4 Conditions

When limited inquiry is initiated by a Bluetooth device, it shall be in the INQUIRY state for at least $T_{\text{GAP}}(100)$ and perform inquiry using the LIAC.

In order to receive inquiry response, the remote devices in range has to be made limited discoverable.



6.3 NAME DISCOVERY

6.3.1 Purpose

The purpose of name discovery is to provide the initiator with the Bluetooth Device Name of connectable devices (i.e., . devices in range that will respond to paging).

6.3.2 Term on UI level

“Bluetooth Device Name Discovery”.

6.3.3 Description

6.3.3.1 Name request

Name request is the procedure for retrieving the Bluetooth Device Name from a connectable Bluetooth device. It is not necessary to perform the full link establishment procedure (see [Section 7.1](#)) in order to just to get the name of another device.

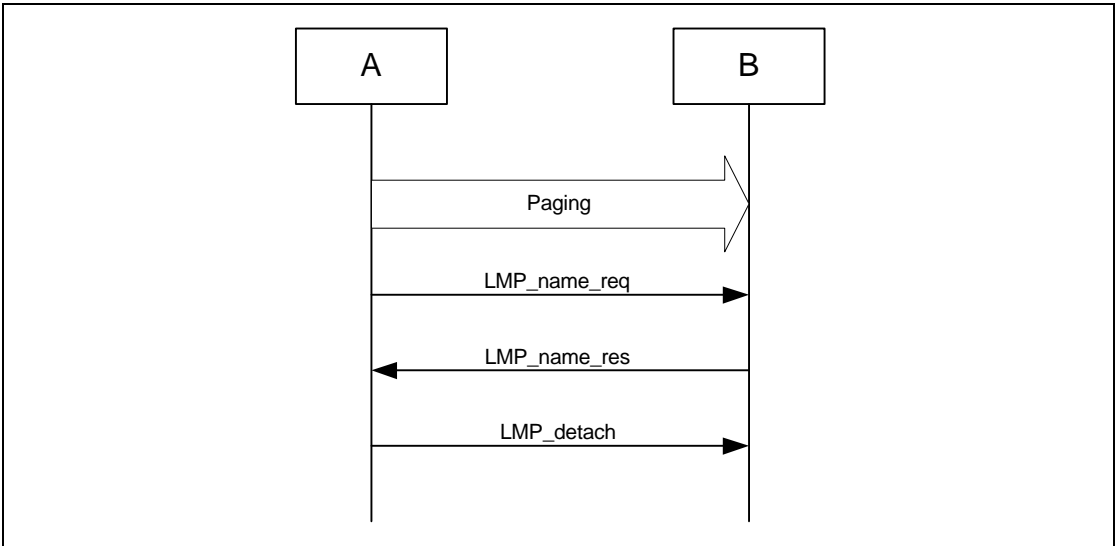


Figure 6.3: Name request procedure.

6.3.3.2 Name discovery

Name discovery is the procedure for retrieving the Bluetooth Device Name from connectable Bluetooth devices by performing name request towards known devices (i.e., . Bluetooth devices for which the Bluetooth Device Addresses are available).

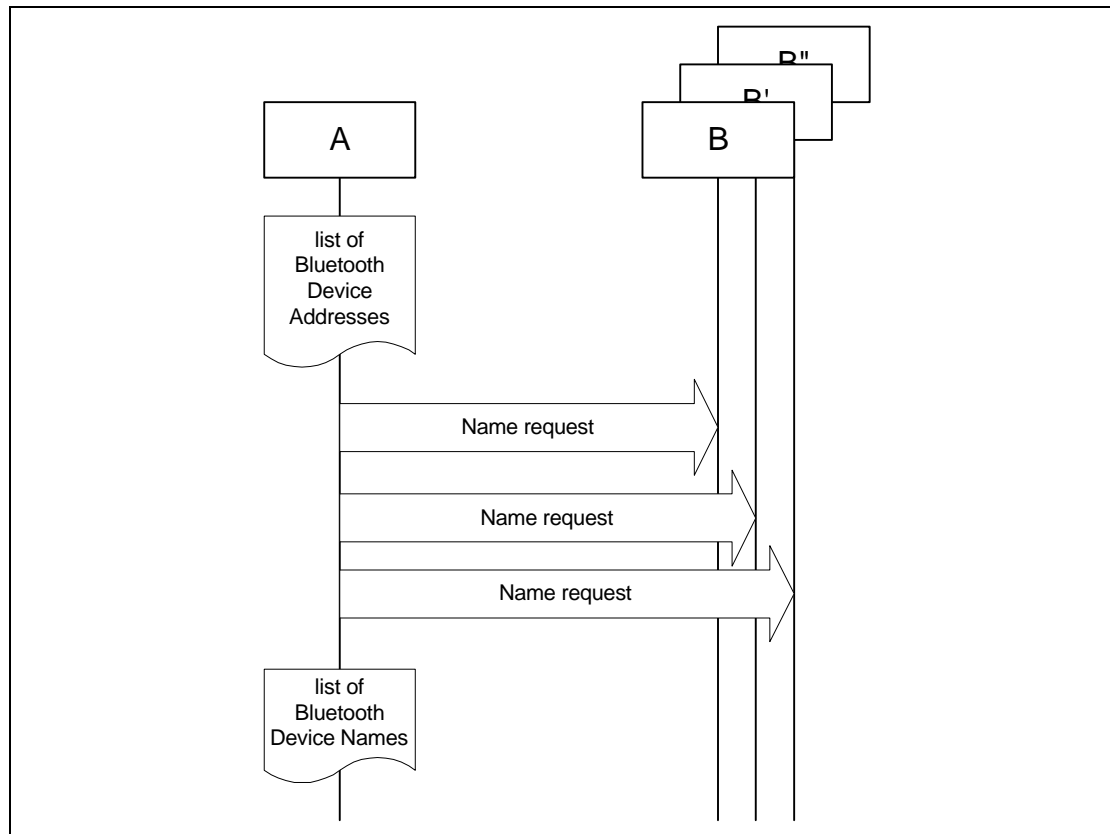


Figure 6.4: Name discovery procedure.

6.3.4 Conditions

The initiator will use the Device Access Code of the remote device as retrieved immediately beforehand, beforehand – normally through an inquiry procedure.

6.4 DEVICE DISCOVERY

6.4.1 Purpose

The purpose of device discovery is to provide the initiator with the Bluetooth Address, clock, Class of Device, used page scan mode and Bluetooth device name of discoverable devices.

6.4.2 Term on UI level

“Bluetooth Device Discovery”.

6.4.3 Description

During the device discovery procedure, first an inquiry (either general or limited) is performed performed, and then name discovery is done towards some or all of the devices that responded to the inquiry.

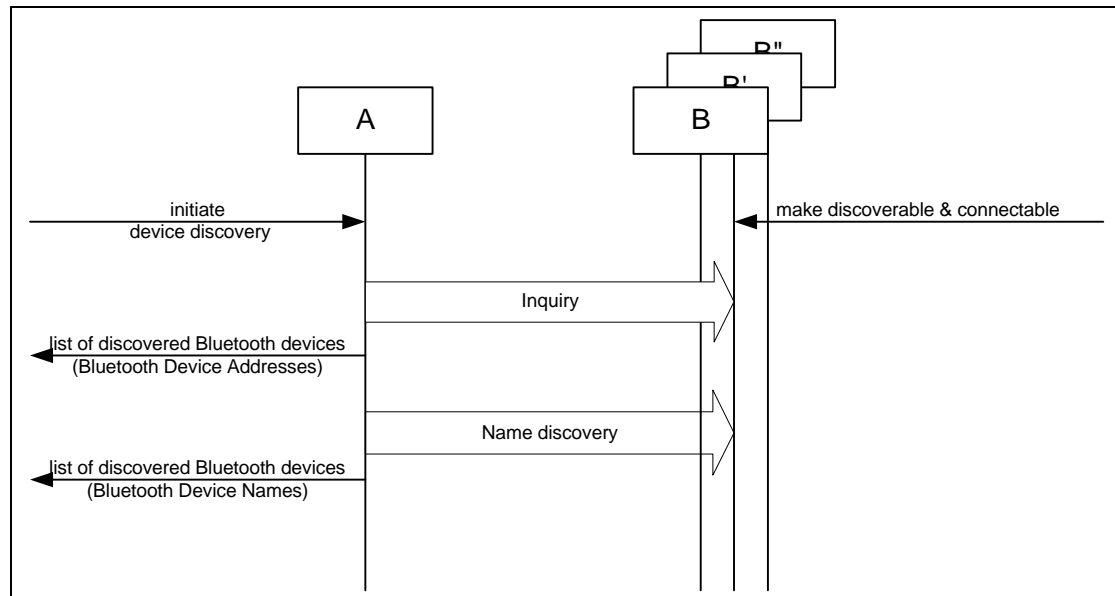


Figure 6.5: Device discovery procedure.

6.4.4 Conditions

Conditions according to for both inquiry (general or limited) and name discovery must be fulfilled (i.e. devices discovered during device discovery must be both discoverable and connectable).

6.5 BONDING

6.5.1 Purpose

The purpose of bonding is to create a relation between two Bluetooth devices based on a common link key (a bond). The link key is created and exchanged (pairing) during the bonding procedure and is expected to be stored by both Bluetooth devices and devices, to be used for future authentication.

In addition to pairing, the bonding procedure can involve higher layer initialisation initialization procedures.

6.5.2 Term on UI level

“Bluetooth Bonding”

6.5.3 Description

Two aspects of the bonding procedure are described here. Dedicated bonding is what is done when the two devices **are** explicitly **are** set to perform only a creation and exchange of a common link key.

General bonding is included to indicate that the framework for the dedicated bonding procedure is the same as found in the normal channel and connection establishment procedures. This means that pairing may be performed successfully if A has initiated bonding while B is in its normal connectable and security modes.

The main difference with **bonding bonding**, as compared to a pairing done during link or channel **establishment establishment**, is that for bonding it is the paging device (A) that must initiate the authentication.

6.5.3.1 General bonding

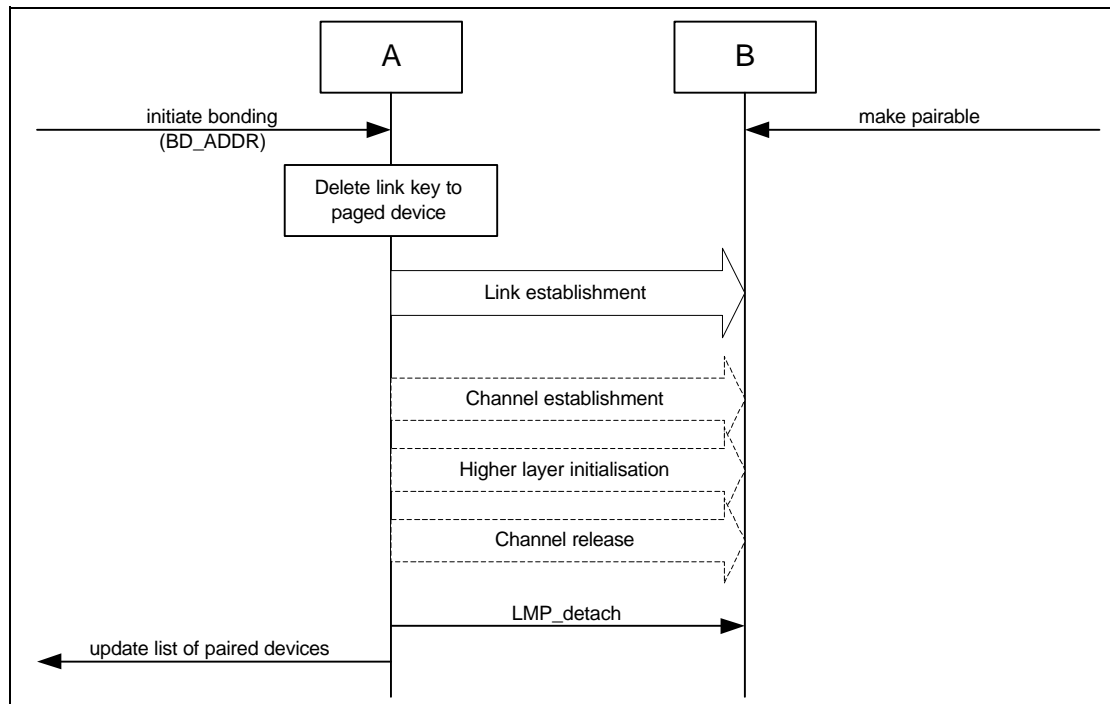


Figure 6.6: General description of bonding as being the link establishment procedure executed under specific conditions on both **devices devices**, followed by an optional higher layer **initialisation initialization** process.

6.5.3.2 Dedicated bonding

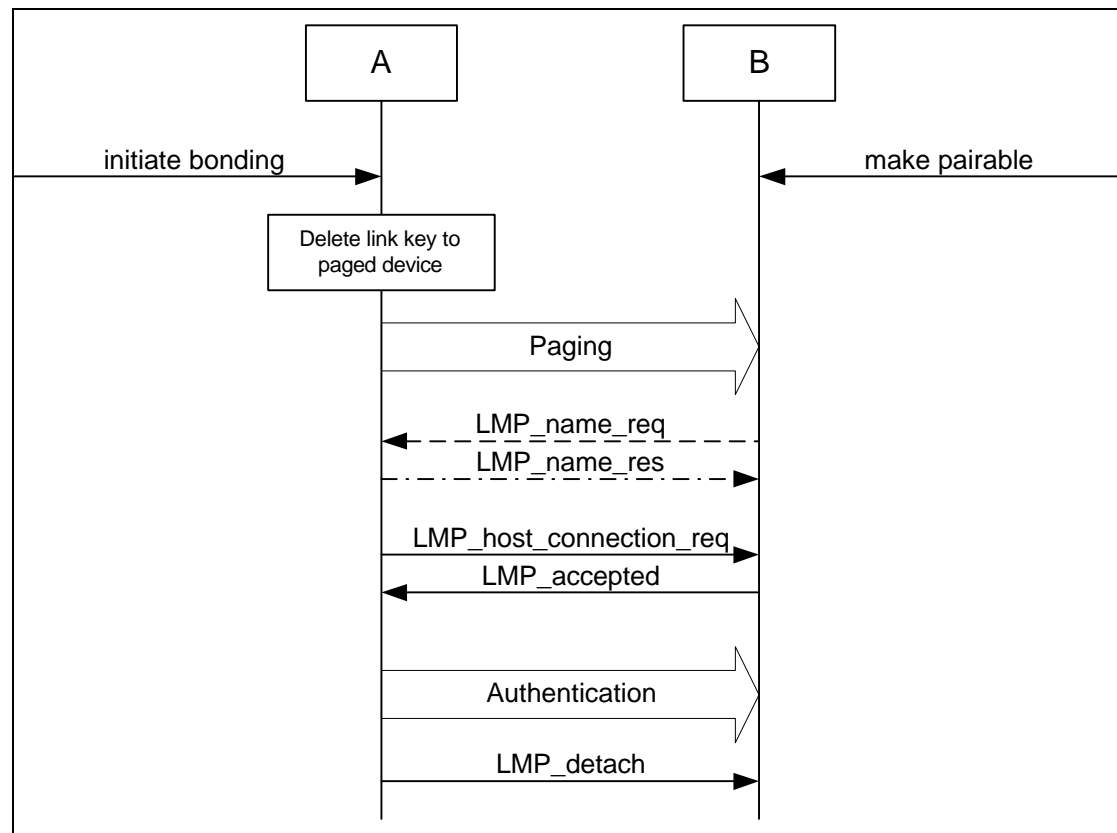


Figure 6.7: Bonding as performed when the purpose of the procedure is only to create and exchange a link key between two Bluetooth devices.

6.5.4 Conditions

Before bonding can be initiated, the initiating device (A) must know the Device Access Code of the device to pair with. This is normally done by first performing device discovery. A Bluetooth Device that can initiate bonding (A) should use limited inquiry inquiry, and a Bluetooth Device that accepts bonding (B) should support the limited discoverable mode.

Bonding is in principle the same as link establishment with the conditions:

- The paged device (B) shall be set into pairable mode. The paging device (A) is assumed to allow pairing since it has initiated the bonding procedure.
- The paging device (the initiator of the bonding procedure, A) shall initiate authentication.
- Before initiating the authentication part of the bonding procedure, the paging device should delete any link key corresponding to a previous bonding with the paged device.
- If the paging device does not intend to initiate any higher layer initialisation initialization during bonding, it need not send LMP_host_request before initiating authentication.



7 ESTABLISHMENT PROCEDURES

	Procedure	Ref.	Support in A	Support in B
1	Link establishment	7.1	M	M
2	Channel establishment	7.2	O	M
3	Connection establishment	7.3	O	O

Table 7.1: Establishment procedures

The establishment procedures defined here do not include any discovery part. Before establishment procedures are initiated, the information provided during device discovery (in the FHS packet of the inquiry response or in the response to a name request) has to be available in the initiating device. This information is:

- The Bluetooth Device Address (BD_ADDR) from which the Device Access Code is generated;
- The system clock of the remote device;
- The page scan mode used by the remote device.

Additional information provided during device discovery that is useful for making the decision to initiate an establishment procedure is:

- The Class of device;
- The Device name.

7.1 LINK ESTABLISHMENT

7.1.1 Purpose

The purpose of the link establishment procedure is to establish a physical link (of ACL type) between two Bluetooth devices using procedures from [1] and [2].

7.1.2 Term on UI level

“Bluetooth link establishment”

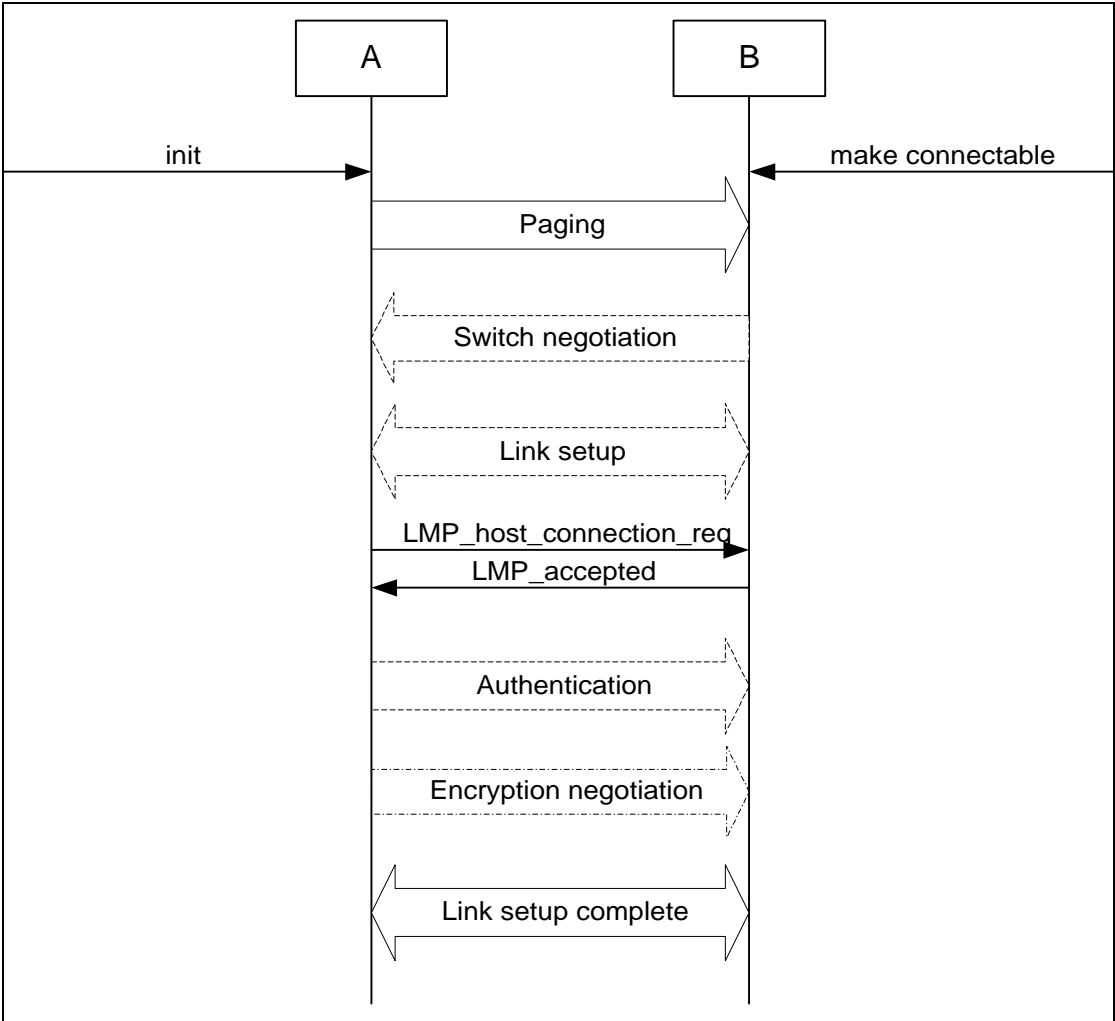
7.1.3 Description

In this sub-section, the paging device (A) is in security mode 3. The paging device cannot during link establishment distinguish if the paged device (B) is in security mode 1 or 2.



7.1.3.1 B in security mode 1 or 2

I



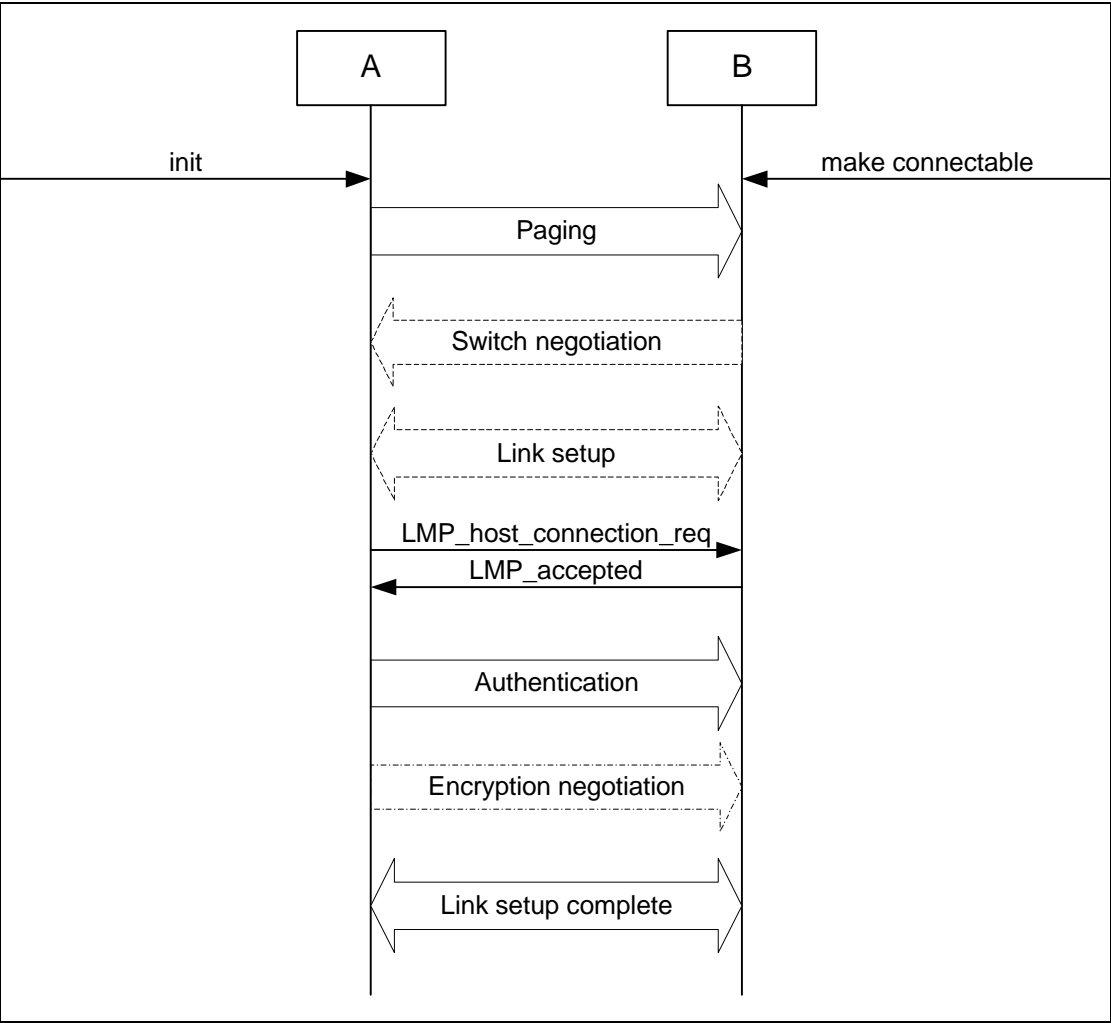
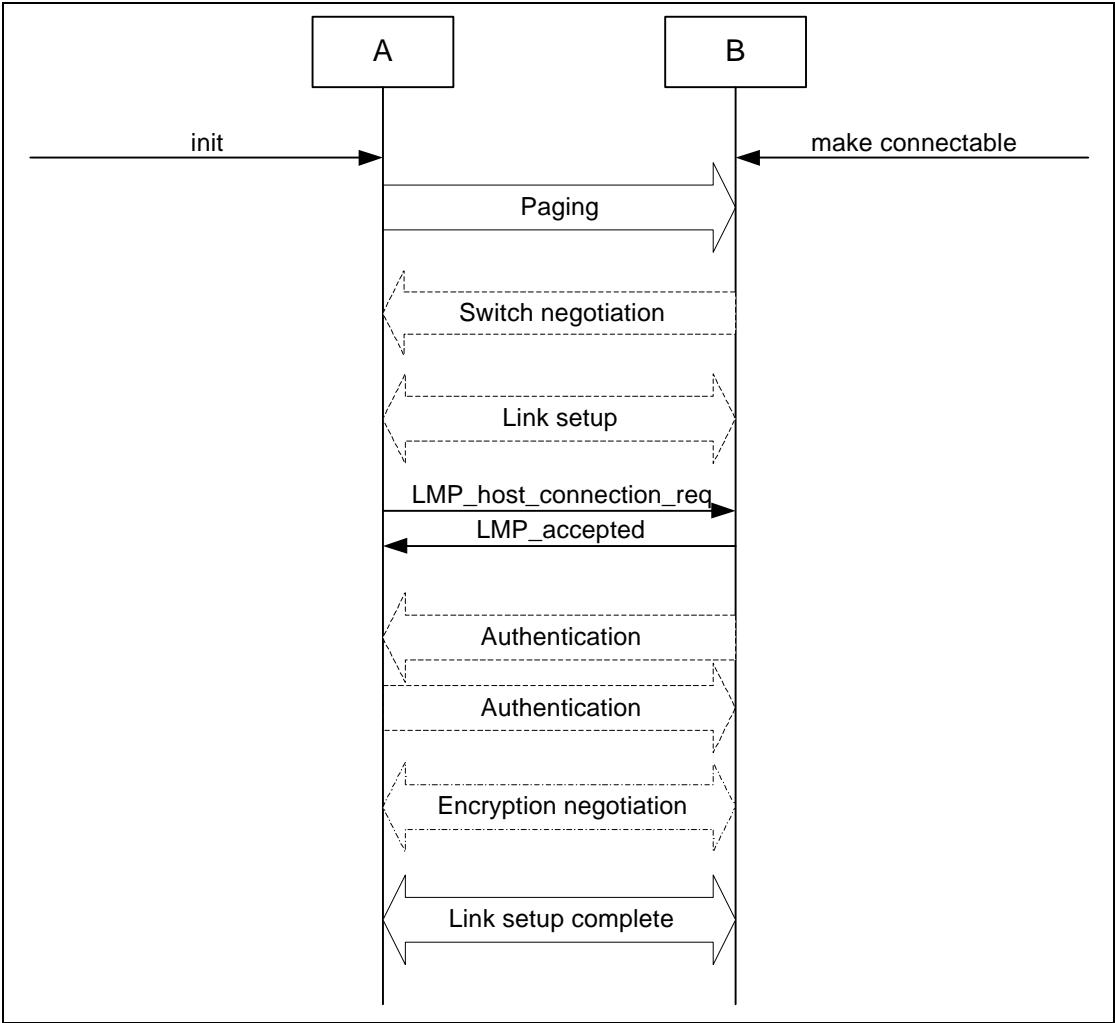


Figure 7.1: Link establishment procedure when the paging device (A) is in security mode 3 and the paged device (B) is in security mode 1 or 2.



7.1.3.2 B in security mode 3

I



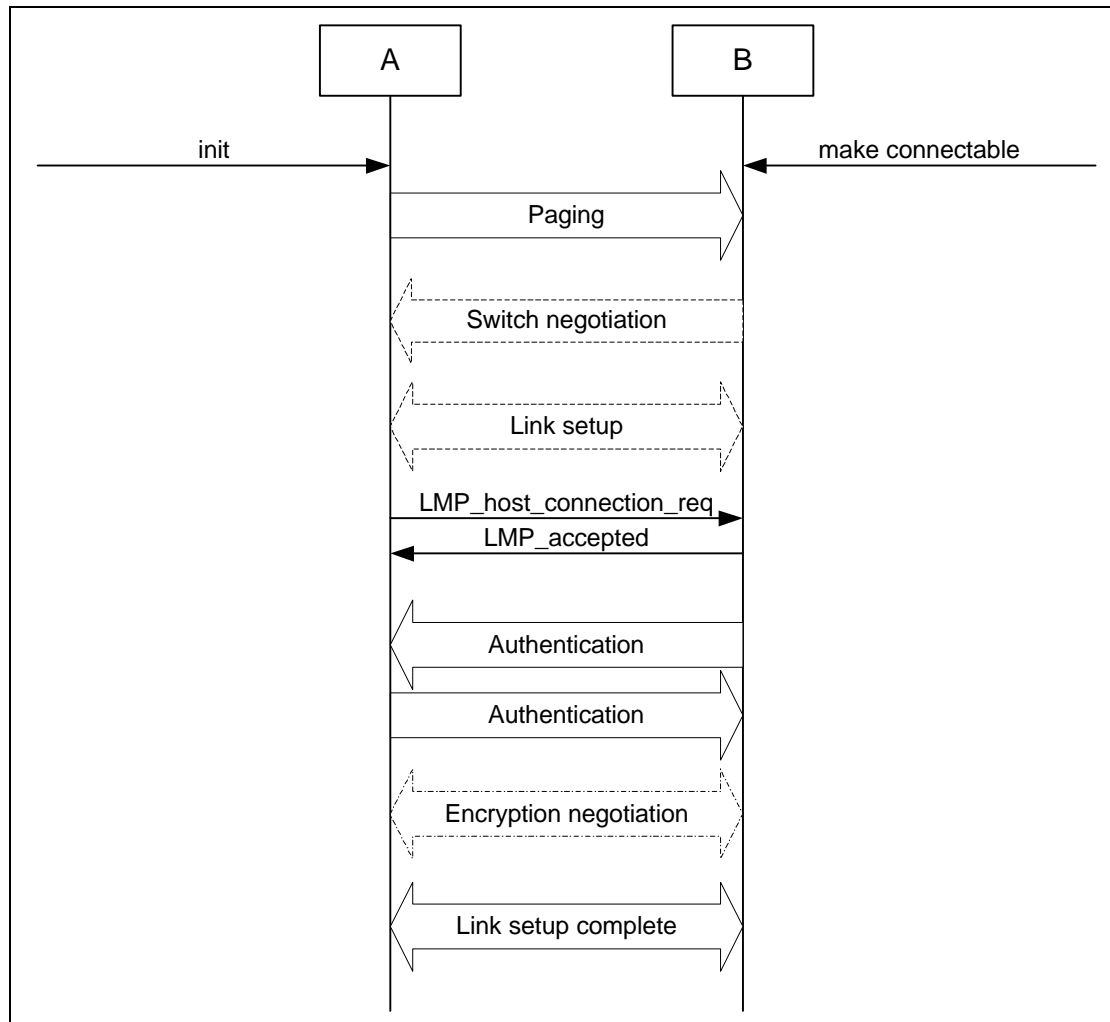


Figure 7.2: Link establishment procedure when both the paging device (A) and the paged device (B) are in security mode 3.

7.1.4 Conditions

The paging procedure shall be according to [1] and the paging device should use the Device access code and page mode received through a previous inquiry. When paging is completed, a physical link between the two Bluetooth devices is established.

If role switching is needed (normally it is the paged device that has an interest to **change in changing** the master/slave roles) it should be done as early as possible after the physical link is established. If the paging device does not accept the switch, the paged device has to consider **if whether** to keep the physical link or not.

Both devices may perform link setup (using LMP procedures that require no interaction with the host on the remote side). Optional LMP features can be used after having confirmed (using LMP_feature_req) that the other device **support supports** the feature.

When the paging device needs to go beyond the link setup phase, it issues a request to be connected to the host of the remote device. If the paged device is in security mode 3, this is the trigger for initiating authentication.



The paging device shall send LMP_host_connection_req during link establishment (i.e., before channel establishment) and may initiate authentication only after having sent LMP_host_connection_request.

Any of the devices can initiate encryption after an authentication has been performed.

After an authentication has been performed, any of the devices can initiate encryption.

Further link configuration may take place after the LMP_host_connection_req and when LMP_host_connection_req. When both devices are satisfied, they send LMP_setup_complete.

Link establishment is completed when both devices have sent LMP_setup_complete.

7.2 CHANNEL ESTABLISHMENT

7.2.1 Purpose

The purpose of the channel establishment procedure is to establish a Bluetooth channel (a logical link) between two Bluetooth devices using [3].

7.2.2 Term on UI level

“Bluetooth channel establishment”.

7.2.3 Description

In this sub-section, the initiator (A) is in security mode 3. The During channel establishment, the initiator cannot during channel establishment distinguish if the acceptor (B) is in security mode 1 or 3.

7.2.3.1 *B in security mode 2*

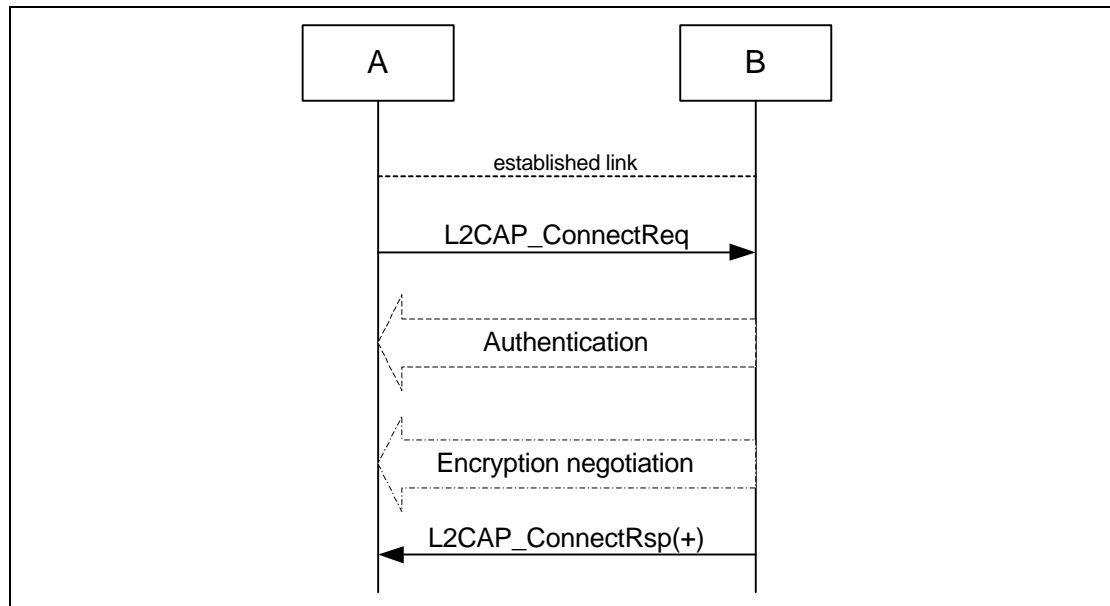


Figure 7.3: Channel establishment procedure when the initiator (A) is in security mode 3 and the acceptor (B) is in security mode 2.

7.2.3.2 *B in security mode 1 or 3*

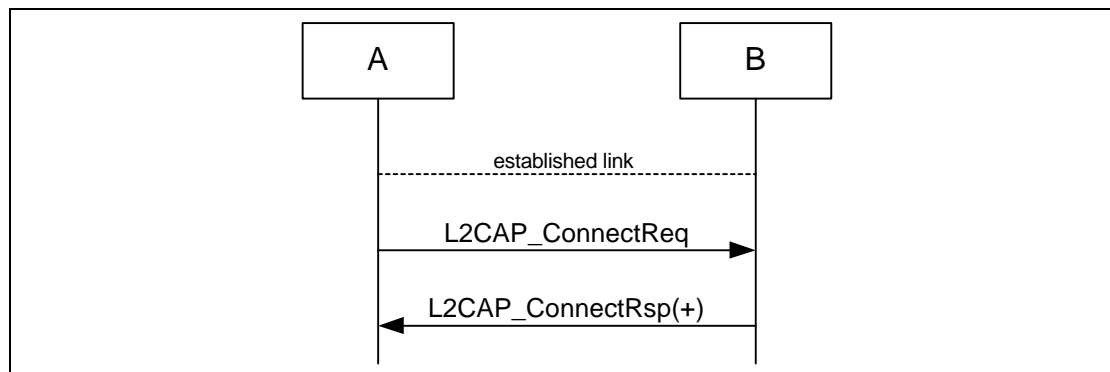


Figure 7.4: Channel establishment procedure when the initiator (A) is in security mode 3 and the acceptor (B) is in security mode 1 or 3.

7.2.4 Conditions

Channel establishment starts after link establishment is completed when the initiator sends a channel establishment request (L2CAP_ConnectReq).

Depending on security **mode**, security procedures may take place after the channel establishment has been initiated.

Channel establishment is completed when the acceptor responds to the channel establishment request (with a positive L2CAP_ConnectRsp).



7.3 CONNECTION ESTABLISHMENT

7.3.1 Purpose

The purpose of the connection establishment procedure is to establish a connection between applications on two Bluetooth devices.

7.3.2 Term on UI level

“Bluetooth connection establishment”

7.3.3 Description

In this sub-section, the initiator (A) is in security mode 3. **The During connection establishment, the** initiator cannot **during connection establishment** distinguish if the acceptor (B) is in security mode 1 or 3.

7.3.3.1 B in security mode 2

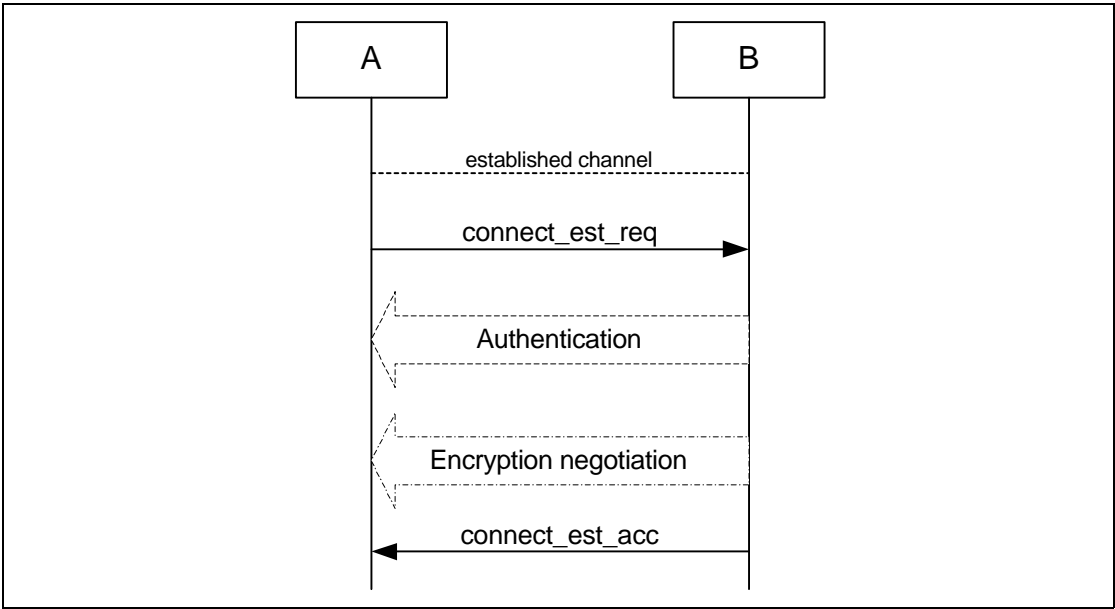


Figure 7.5: Connection establishment procedure when the initiator (A) is in security mode 3 and the acceptor (B) is in security mode 2.

7.3.3.2 B in security mode 1 or 3

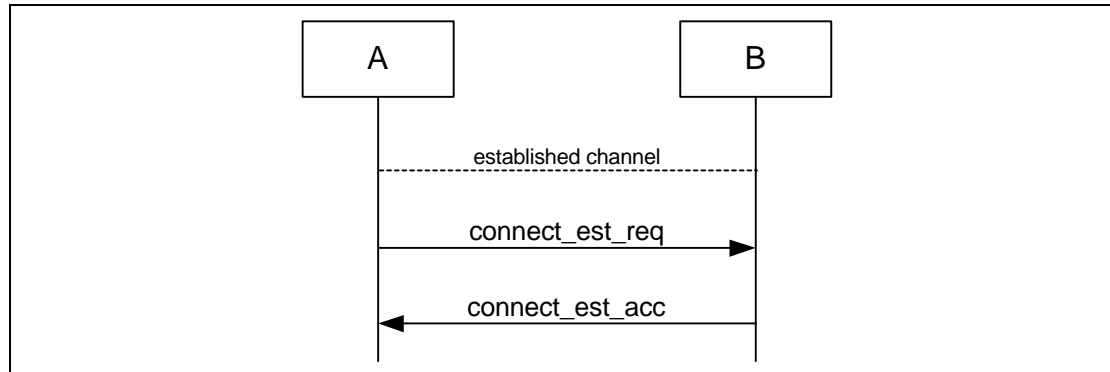


Figure 7.6: Connection establishment procedure when the initiator (A) is in security mode 3 and the acceptor (B) is in security mode 1 or 3.

7.3.4 Conditions

Connection establishment starts after channel establishment is **completed**, when the initiator sends a connection establishment request (“connect_est_req” is application **protocol** protocol-dependent). This request may be a TCS SETUP message [5] in the case of a Bluetooth telephony application **Cordless Telephony Profile** or **initialisation** **Cordless Telephony Profile**, or **initialization** of RFCOMM and establishment of DLC [4] in the case of a serial **port** port-based application **Serial Port Profile** **Serial Port Profile** (although neither TCS or RFCOMM use the term “connection” for this).

Connection establishment is completed when the acceptor accepts the connection establishment request (“connect_est_acc” is application protocol dependent).

7.4 ESTABLISHMENT OF ADDITIONAL CONNECTION

When a Bluetooth device has established one connection with another Bluetooth device, it may be available for establishment of:

- A second connection on the same **channel** **channel**, and/or
- A second channel on the same **link** **link**, and/or
- A second physical link.

If the new establishment procedure is to be towards the same device, the security part of the establishment depends on the security modes used. If the new establishment procedure is to be towards a new remote device, the device should behave according to active modes independent of the fact that it already has another physical link established (unless allowed co-incident radio and baseband events **has** **have** to be handled).



8 DEFINITIONS

In the following, terms written with capital letters refer to states.

8.1 GENERAL

8.2 GENERAL DEFINITIONS

Mode A set of directives that defines how a device will respond to certain events.

Idle As seen from a remote device, a Bluetooth device is idle, or is in idle mode, when there is no link established between them.

Bond A relation between two Bluetooth devices defined by creating, exchanging and storing a common link key. The bond is created through the bonding or **lmpLMP**-pairing procedures.

8.3 CONNECTION RELATED

8.4 CONNECTION-RELATED DEFINITIONS

Physical channel A synchronized Bluetooth baseband-compliant RF hopping sequence.

Piconet A set of Bluetooth devices sharing the same physical channel defined by the master parameters (clock and BD_ADDR).

Physical link A **Baseband Baseband**-level connection¹ between two devices established using paging. A physical link comprises a sequence of transmission slots on a physical channel alternating between master and slave transmission slots.

ACL link An asynchronous (packet-switched) **connection² connection¹** between two devices created on LMP level. Traffic on an ACL link uses ACL packets to be transmitted.

SCO link A synchronous (circuit-switched) **connection³ connection¹** for reserved bandwidth communications, ; e.g., **voice, . voice** between two **devices devices**, created on **the** LMP level by reserving slots periodically on a physical channel. Traffic on an SCO link uses SCO packets to be transmitted. SCO links can be established only after an ACL link has first been established.

1. The term "connection" used here is not identical to the definition below but below. It is used due to in the absence of a lack of better terms.more concise term.

2. The term "connection" used here is not identical to the definition below but is used due to a lack of better terms.

3. The term "connection" used here is not identical to the definition below but is used due to a lack of better terms.



Link Shorthand for an ACL link.

PAGE A baseband state where a device transmits page trains, and processes any eventual responses to the page trains.

PAGE_SCAN A baseband state where a device listens for page trains.

Page The transmission by a device of page trains containing the Device Access Code of the device to which the physical link is requested.

Page scan The listening by a device for page trains containing its own Device Access Code.

Channel A logical connection on L2CAP level between two devices serving a single application or higher layer protocol.

Connection A connection between two peer applications or higher layer protocols mapped onto a channel.

Connecting A phase in the communication between devices when a connection between them is being established. (Connecting phase follows after the link establishment phase is completed.)

Connect (to service) The establishment of a connection to a service. If not already done, this includes establishment of a physical link, link and channel as well.

8.5 DEVICE RELATED

8.6 DEVICE-RELATED DEFINITIONS

Discoverable device A Bluetooth device in range that will respond to an inquiry (normally in addition to responding to page).

Silent device A Bluetooth device appears as silent to a remote device if it does not respond to inquiries made by the remote device. A device may be silent due to being non-discoverable or due to baseband congestion while being discoverable.

Connectable device A Bluetooth device in range that will respond to a page.

Trusted device A paired device that is explicitly marked as trusted.

Paired device A Bluetooth device with which a link key has been exchanged (either before connection establishment was requested or during connecting phase).

Pre-paired device A Bluetooth device with which a link key was exchanged, and the link key is stored, before link establishment.

Un-paired device A Bluetooth device for which there was no exchanged link key available before connection establishment was request.



Known device A Bluetooth device for which at least the BD_ADDR is stored.

Un-known device A Bluetooth device for which no information (**neither** BD_ADDR, link key or other) is stored.

Authenticated device A Bluetooth device whose identity has been verified during the lifetime of the current **link link**, based on the authentication procedure.

8.7 PROCEDURE RELATED

8.8 PROCEDURE-RELATED DEFINITIONS

Paging A procedure for establishing a physical link of ACL type on baseband **level level**, consisting of a page action of the initiator and a page scan action of the responding device.

Link establishment A procedure for establishing a link on LMP level. A link is established when both devices have agreed that LMP setup is completed.

Channel establishment A procedure for establishing a channel on L2CAP level.

Connection establishment A procedure for creating a connection mapped onto a channel.

Creation of a trusted relationship A procedure where the remote device is marked as a trusted device. This includes storing a common link key for future authentication and pairing (if the link key is not available).

Creation of a secure connection. A procedure of establishing a connection, including authentication and encryption.

Device discovery A procedure for retrieving the Bluetooth device address, clock, **class of class-of-device** field and used page scan mode from discoverable devices.

Name discovery A procedure for retrieving the user-friendly name (the Bluetooth device name) of a connectable device.

Service discovery Procedures for querying and browsing for services offered by or through another Bluetooth device.

8.9 SECURITY RELATED

8.10 SECURITY-RELATED DEFINITIONS

Authentication A generic procedure based on **lmpLMP**-authentication if a link key exists or on **lmpLMP**-pairing if no link key exists.

lmpLMP-authentication An LMP level procedure for verifying the identity of a remote device. The procedure is based on a challenge-response mechanism using a ran-



dom number, a secret key and the BD_ADDR of the non-initiating device. The secret key used can be a previously exchanged link key or an **initialisation initialization** key created based on a PIN (as used when pairing).

Authorisation A procedure where a user of a Bluetooth device grants a specific (remote) Bluetooth device access to a specific service. Authorisation implies that the identity of the remote device can be verified through authentication.

Authorization A procedure where a user of a Bluetooth device grants a specific (remote) Bluetooth device access to a specific service. Authorization implies that the identity of the remote device can be verified through authentication.

Authorize The act of granting a specific Bluetooth device access to a specific service. It may be based **on upon** user **confirmation confirmation**, or **given the** existence of a trusted relationship.

The act of granting a specific Bluetooth device access to a specific service. It may be based on user confirmation or existence of a trusted relationship.

ImpLMP-pairing A procedure that authenticates two **devices devices**, based on a **PIN PIN**, and subsequently creates a common link key that can be used as a basis for a trusted relationship or a (single) secure connection. The procedure consists of the steps: creation of an **initialisation initialization** key (based on a random number and a PIN), **ImpLMP**-authentication based on the **initialisation initialization** key and creation of a common link key.

Bonding A dedicated procedure for performing the first **authentication authentication**, where a common link key is created and stored for future use.

Trusting The marking of a paired device as trusted. Trust marking can be done by the **user user**, or automatically by the device (e.g. when in pairable mode) after a successful pairing.

9 ANNEX A (NORMATIVE): TIMERS AND CONSTANTS

The following timers are required by this profile.

Timer name	Recommended value	Description	Comment
$T_{\text{GAP}}(100)$	10.24 s	Normal time span that a Bluetooth device performs inquiry.	Used during inquiry and device discovery.
$T_{\text{GAP}}(101)$	10.625 ms	Minimum time in INQUIRY_SCAN.	A discoverable Bluetooth device enters INQUIRY_SCAN for at least $T_{\text{GAP}}(101)$ every $T_{\text{GAP}}(102)$.
$T_{\text{GAP}}(102)$	2.56 s	Maximum time between repeated INQUIRY_SCAN enterings.	Maximum value of the inquiry scan interval, $T_{\text{inquiry scan}}$.
$T_{\text{GAP}}(103)$	30.72 s	A Bluetooth device shall not be in a discoverable mode less than $T_{\text{GAP}}(103)$.	Minimum time to be discoverable.
$T_{\text{GAP}}(104)$	1 min	A Bluetooth device should not be in limited discoverable mode more than $T_{\text{GAP}}(104)$.	Recommended upper limit.

Table 9.1: Defined GAP timers



10 ANNEX B (INFORMATIVE): INFORMATION FLOWS OF RELATED PROCEDURES

10.1 LMP-AUTHENTICATION

The specification of authentication on link level is found in [\[2\]](#).

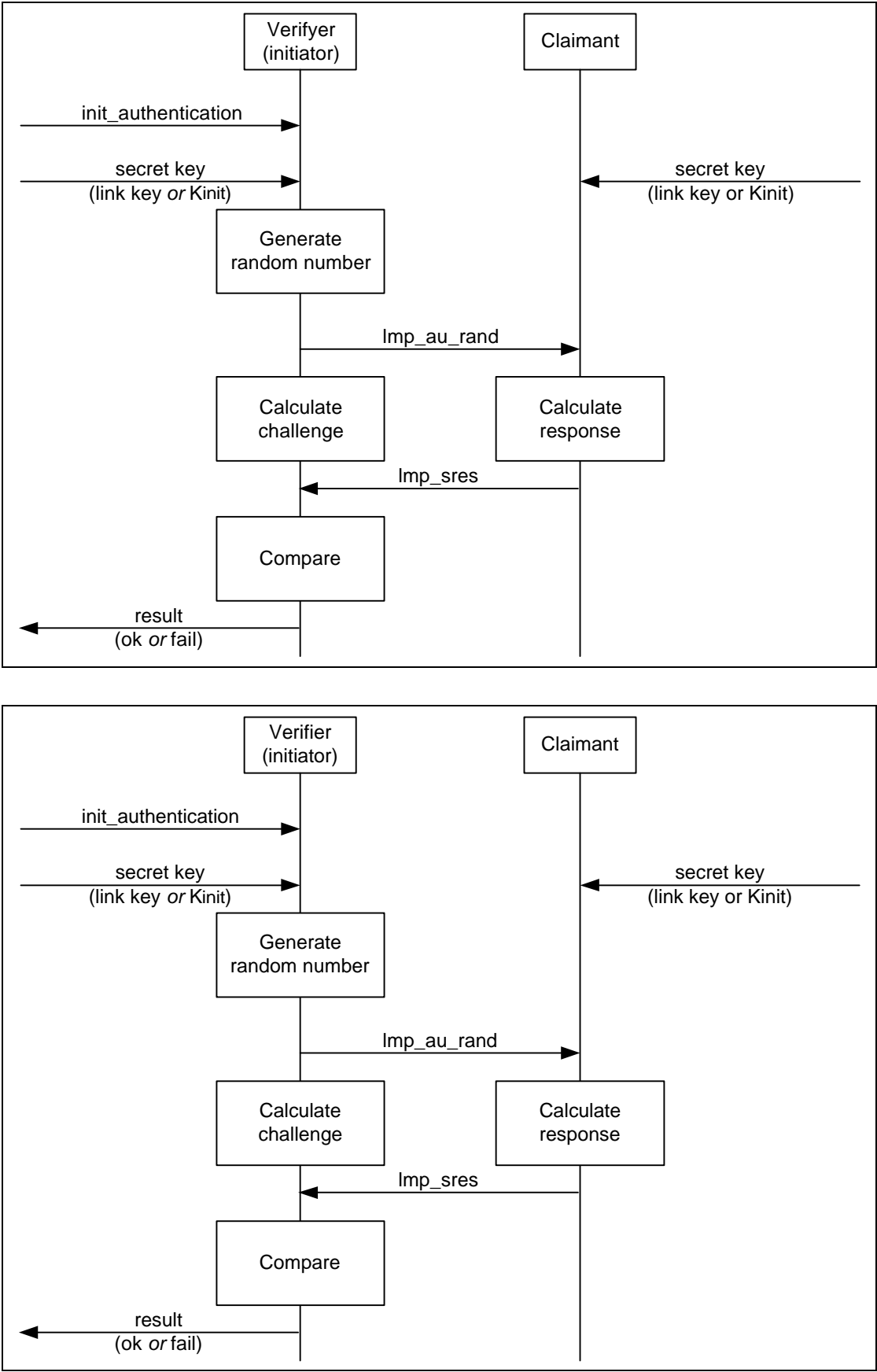


Figure 10.1: *ImpLMP*-authentication as defined by [2].



The secret key used here may be either an already exchanged link key or an **initialisation initialization** key created in the **lmpLMP**-pairing procedure.



10.2 LMP-PAIRING

The specification of pairing on link level is found in [\[2\]](#).

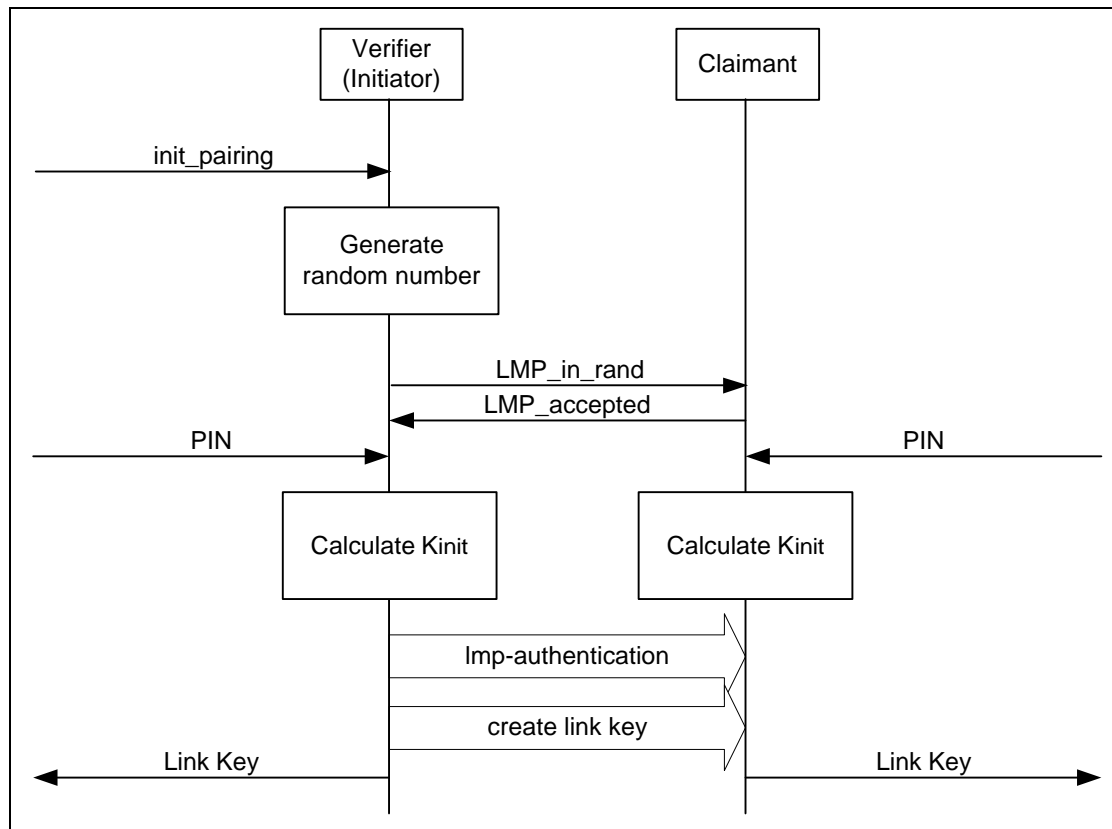
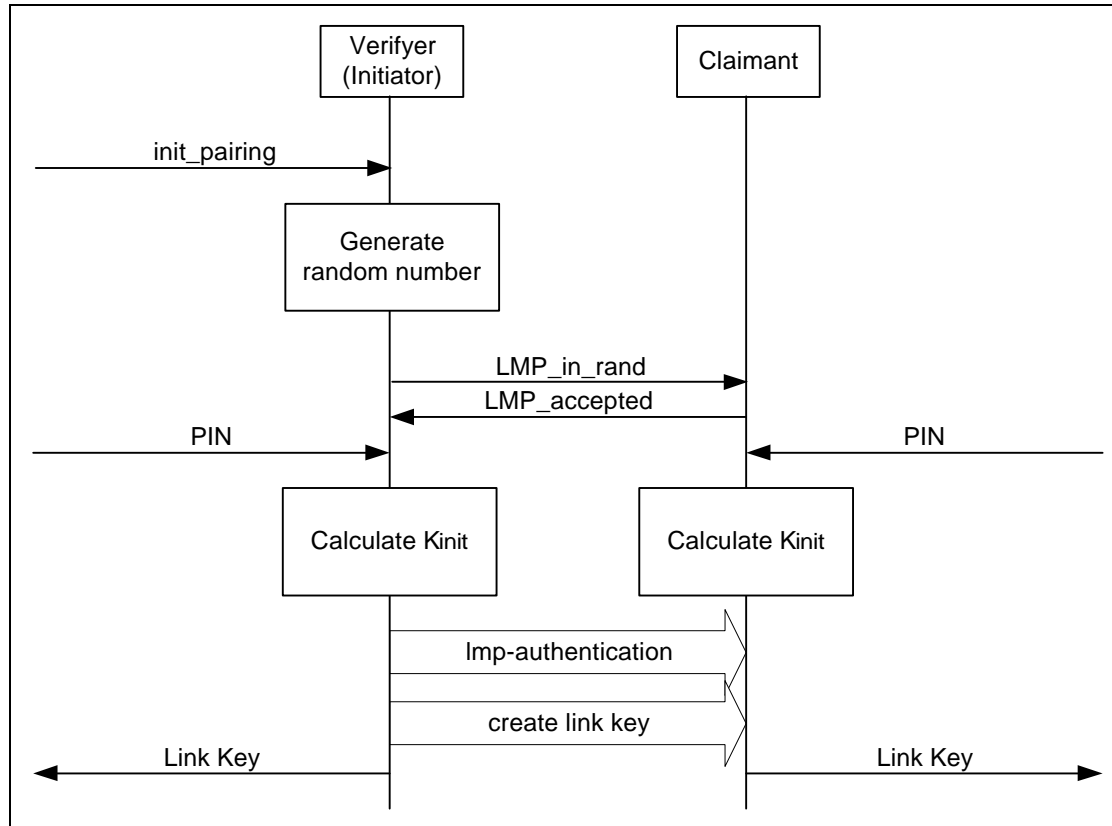


Figure 10.2: *lmpLMP*-pairing as defined in [2].



The PIN used here is PN_{BB} .

The create link key procedure is described in section 3.3.4 of [2] and section 14.2.2 of [1]. In case the link key is based on a combination key, a mutual authentication takes place and shall be performed irrespective of current security mode.

10.3 SERVICE DISCOVERY

The service discovery protocol **Service Discovery Protocol** [6] specifies what PDUs are used over-the-air to inquire about services and service attributes. The procedures for discovery of supported services and capabilities using the **service discovery protocol Service Discovery Protocol** are described in the **Service Discovery Application ProfileService Discovery Application Profile**. This is just an example.

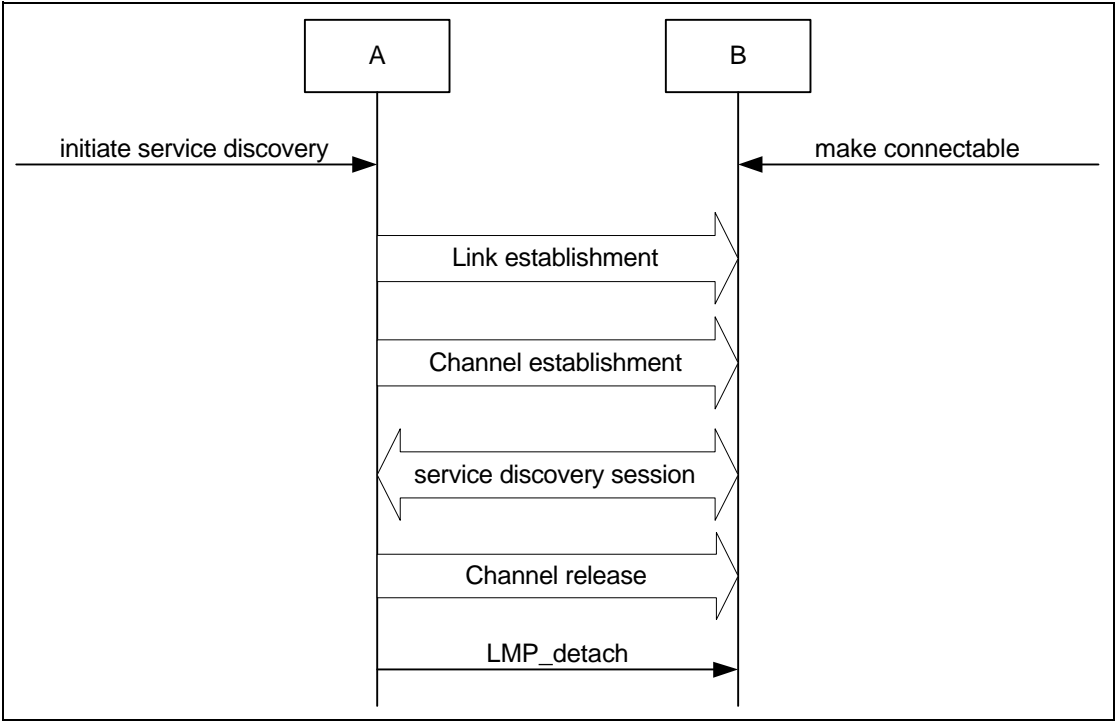


Figure 10.3: Service discovery procedure.



11 REFERENCES

- [1] Bluetooth Baseband Specification
- [2] Bluetooth Link Manager Protocol
- [3] Bluetooth Logical Link Control and Adaptation Protocol
- [4] Bluetooth RFCOMM
- [5] Bluetooth Telephony Control Specification
- [6] Bluetooth Service Discovery Protocol
- [7] Bluetooth Service Discovery Application Profile
- [8] Bluetooth Cordless Telephony Profile
- [9] Bluetooth Serial Port Profile
- [10] Bluetooth Security Architecture (white paper)
- [11] Bluetooth Assigned Numbers