BLUETOOTH™ SECURITY WHITE PAPER

Bluetooth SIG Security Expert Group

Abstract

This document describes the usage of Bluetooth Security as well as additional security mechanisms for selected Bluetooth wireless profiles.

Special Interest Group (SIG)

The following companies are represented in the Bluetooth Special Interest Group:

3Com Corporation
Ericsson Technology Licensing AB
IBM Corporation
Intel Corporation
Agere Systems, Inc.
Microsoft Corporation
Motorola, Inc.
Nokia Corporation
Toshiba Corporation

Revision History

Revision	Date	Comments
0.5	2001-10-22	First version based on content from a previous white paper proposal.
0.6	2001-11-06	Reference list updated. Minor editorial changes and changes related to the protection of the Bluetooth trademark.
0.9	2001-11-28	After recommendations from the BARB, a short section with general recommendations has been added. Minor editorial changes based on received comments from the second BARB review.

Contributors

Brant Thomsen	3Com Corporation
Thomas Baker	Agere Systems, Inc.
Simon Blake-Wilson	Certicom
Dan Willey	Certicom
Thomas Xydis	Ensure Technologies
Christian Gehrmann	Ericsson Technology Licensing AB
Georges Seuron	IBM Corporation
Bill Austin	Motorola, Inc.
George Muncaster	Motorola, Inc.
Kaisa Nyberg	Nokia Corporation
Susanne Wetzel	RSA Security, Inc.
Jan-Ove Larsson	RSA Security, Inc.

Disclaimer and Copyright Notice

Contents

1 Introduction

The Bluetooth wireless technology provides short-range, wireless connectivity between common devices. Different applications can be built based on these spontaneous, *ad hoc* networks. The security requirements for Bluetooth applications will vary based on the sensitivity of the information involved, the market, and the needs of the user. There are some applications that do not require any security and others which require extremely high levels of security. Risk analysis and trade studies need to be conducted prior to implementing new applications using Bluetooth wireless technology.

The Bluetooth wireless technology system contains a set of *profiles.* A profile defines a selection of messages and procedures (generally termed *capabilities*) from the Bluetooth Specifications. This gives an unambiguous description of the air interface for specified services and use cases. Working groups within the Bluetooth SIG define these profiles. The Security Expert Group (BSEG) provides the Bluetooth SIG and associated working groups with expertise regarding all aspects of Bluetooth Security.

Security can be defined by four fundamental elements: availability, access, integrity, and confidentiality. The current Bluetooth Specification defines security at the link level. Application-level security is not specified, allowing application developers the flexibility to select the most appropriate security mechanisms for their particular application. The Security Expert Group focuses on developing general security architecture models.

In this context, this paper provides security architectures for selected Bluetooth wireless profiles. The sample architecture contains detailed security recommendations applicable for the different profiles. Some general recommendations apply to all profiles. We summarize these recommendations in Section 1.2.

1.1 Contribution of this Paper; Sample Security Architectures

A *security architecture* defines the protocols and functionality required to implement the four elements of security within a specific application category. The rules that determine the access rights to different resources on the devices are called the *access policy*. The access policy together with the description of the usage of basic security mechanisms like authentication and encryption make up the *security policy*. The security policy is part of the security architecture for a Bluetooth application profile.

The security architectures can be implemented in many different ways; e.g., using different protocols and ciphers. In order to provide some guidelines, in Sections 3 through 6 we present sample security architectures for the following five common Bluetooth application profiles:

- Service Discovery Application Profile
- Headset Profile
- Dial-up Networking Profile
- LAN Access Profile
- Synchronization Profile

We have chosen the current LAN Access Profile as one reference profile. This profile is about to be replaced by the PAN Profile. Our LAN access sample architecture can be applied also to the new PAN Profile.

Figure 1 depicts the basic Bluetooth wireless profile structure. The profiles listed above are marked in black.

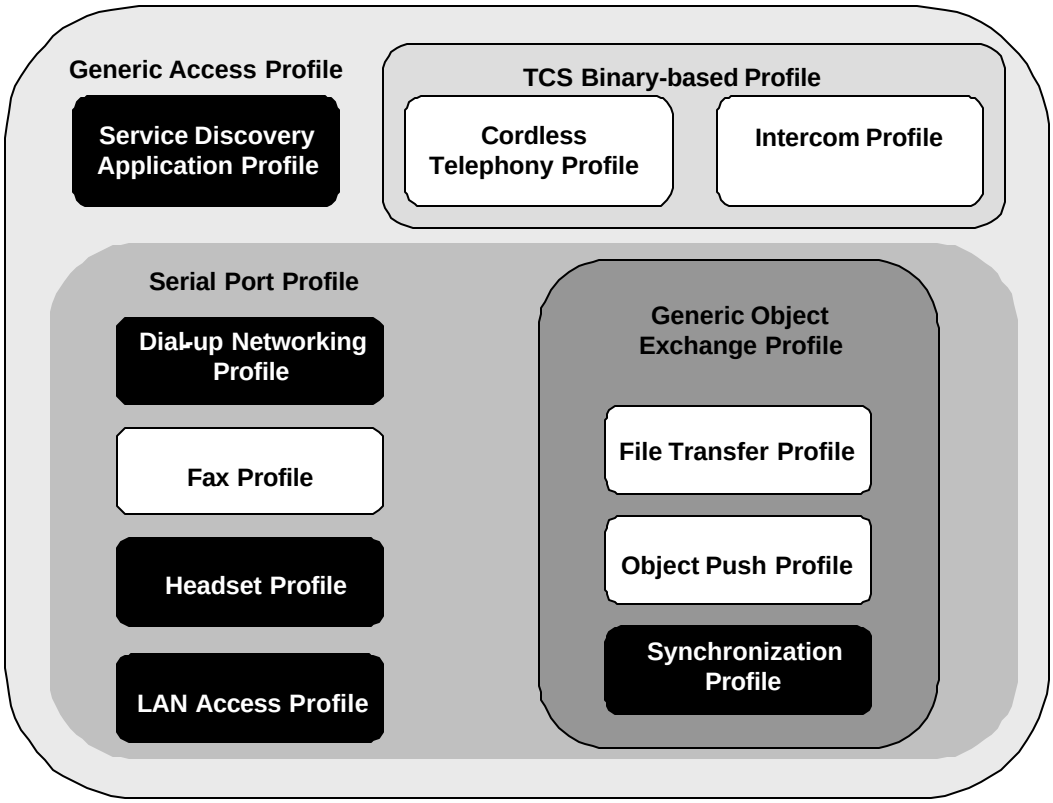

Figure 1: Bluetooth Profiles

It is noted that the solutions described are not mandatory for the different profile implementations.

1.2 General Recommendations

There are some well-known security shortcomings in the current Bluetooth Security concept briefly discussed below.

Based on these shortcomings we make the following general recommendations:

1. Avoid the use of unit keys. Use combination keys instead.
2. Perform bonding in an environment that is as secure as possible against eavesdroppers, and use long random Bluetooth passkeys.

1.2.1 Unit Keys

The authentication and encryption mechanisms based on unit keys are the same as those based on combination keys. However, a unit that uses a unit key is only able to use *one* key for all its secure connections. Hence, it has to *share* this key with all other units that it trusts. Consequently all trusted devices are able to eavesdrop on any traffic based on this key. A trusted unit that has been modified or tampered with could also be able to impersonate the unit distributing the unit key. Thus, when using a unit key there is no protection against attacks from trusted devices.

The Bluetooth combination keys would be much more appropriate to use for almost any Bluetooth unit and therefore we do not recommend the use of unit keys.

1.2.2 Short Passkey Values

During the pairing procedure [1] both units calculate an initialization key. The only secret input to the key calculation is the passkey (PIN). In the next step the combination or unit key is calculated. This calculation is protected using the initialization key. Directly after the exchange of the link key, the authentication procedure is performed. The authentication uses the newly derived link key. All key derivation algorithms are symmetric algorithms that can be implemented in hardware or in software. The computational complexity of the algorithms is not large. Assume that an intruder records all communication during the key exchange and the first authentication between two units. He can then calculate, for each possible passkey value, the corresponding initialization key. Furthermore, for each initialization value, he can calculate the corresponding link key. Finally, for each link key value he can then check the response value for the observed challenge (or he can issue a challenge himself towards the victim device). If he finds a match, he has obtained the correct link key. Since all calculation steps have low complexity, unless the passkey space is large, the intruder can easily compute the correct link key.

As an alternative, the attacker can obtain the passkey and link key by initiating a key exchange with a victim device and perform the same step as described above.

If the attack described above should succeed, the intruder must be present at the pairing occasion and record all communication. Hence, we do not recommend pairing at public places and strongly encourage the use of a long passkey number.

2 Service Discovery Application Profile

Security methods for use with the Bluetooth Service Discovery Application Profile [4] are discussed in this section.

The Service Discovery Application Profile describes the features and procedures used to discover services registered on other Bluetooth wireless devices using the Bluetooth Service Discovery Protocol (SDP). The user, independently of other profiles, specifically initiates the SDP. Service discovery procedures may be associated with other profiles, such as the LAN Access Profile to display network resources. In these situations the security procedures associated with the specific profiles should be applied.

The SDP uses only connection-oriented channels; however, the SDP itself is a connectionless datagram service. It relies on the L2CAP layer to create and manage connections. This is significant in that the basis for security in the SDP is the initial connection and pairing of devices. The SDP itself does not require the use of authentication and/or encryption for SDP transactions. If authentication is performed on the Bluetooth wireless devices to be involved in an SDP procedure, then the devices must pass the authentication test to perform SDP procedures. Therefore, any security procedures applied to the SDP are determined by those used to negotiate the connections between the specific Bluetooth wireless devices. SDP is not available to devices that do not pass this test.

Since SDP security is based on device access to the SDP service, security may be provided by restricting access to trusted devices; i.e., devices with a fixed relationship (paired) that is trusted and has access to services. Presumably the trust relationship is arranged in advance using the Bluetooth pairing mechanism. Once the devices have been paired, SDP is available. No additional security procedures are implemented.

In the case of a connection between untrusted or unknown devices, the service record is freely available, since no security is applied. This, however, is acceptable in many situations since the SDP only provides a record indicating what services are available, not a mechanism to access these services.

3 Headset Profile

This section describes security solutions and usage for the Bluetooth Headset Profile [5].

The security options offered by the current Bluetooth Baseband Specification have been designed for personal devices such as a headset. One important part of Bluetooth secure pairing is the use of a Bluetooth passkey when creating security associations. The security association is used to authenticate and encrypt all communication between two Bluetooth wireless devices. Adequate implementation of Bluetooth Security and Bluetooth passkey can also prevent illegal use of a stolen headset. An example implementation with good security properties is presented.

3.1 Headset Security Model

3.1.1 Architecture

As shown in Figure 1, the Headset Profile depends on both the Serial Port Profile and the Generic Access Profile. The Serial Port Profile provides RS-232 serial cable emulation for Bluetooth wireless devices. The Generic Access Profile (GAP) [1] describes several security aspects of Bluetooth wireless connections. Since the Headset Profile inherits characteristics from the GAP, these aspects also apply to the Headset Profile.

A typical headset configuration consists of two devices, a Headset (HS) and an Audio Gateway (AG) as shown in Figure 2. The AG is typically a cellular phone, laptop, PC, or any other type of audio player device, such as a radio, CD player, etc. For reasons which include personal privacy and preventing infringement on others, it is recommended that communication between the HS and AG be protected by the Bluetooth Baseband [1] authentication and encryption mechanisms. How and when these mechanisms should be used is determined by policy rules, which may be preset or configurable by the end user. In order to set up secure connections, the HS and AG need to store the necessary Bluetooth passkeys and link keys.

Since the HS will normally not have a user interface, it is appropriate to assume that an external device, such as the AG, may control some of the basic settings of the HS (volume, list of approved – e.g., owned or shared – devices to be connected, respective Bluetooth passkey values, etc.). Apart from the pure authentication, encryption, and key storage functions, the HS and AG entities need to use an access policy to provide, for example, for audio connections and for the remote control of the HS.

To provide alternative means for modifying AG and HS functionality, such as application program updates, security access or control policy changes, etc., the device manufacturer may provide a serial port interface. Use of such a wired means of connection to the AG or HS provides a highly secure method of initializing or modifying device operating parameters.

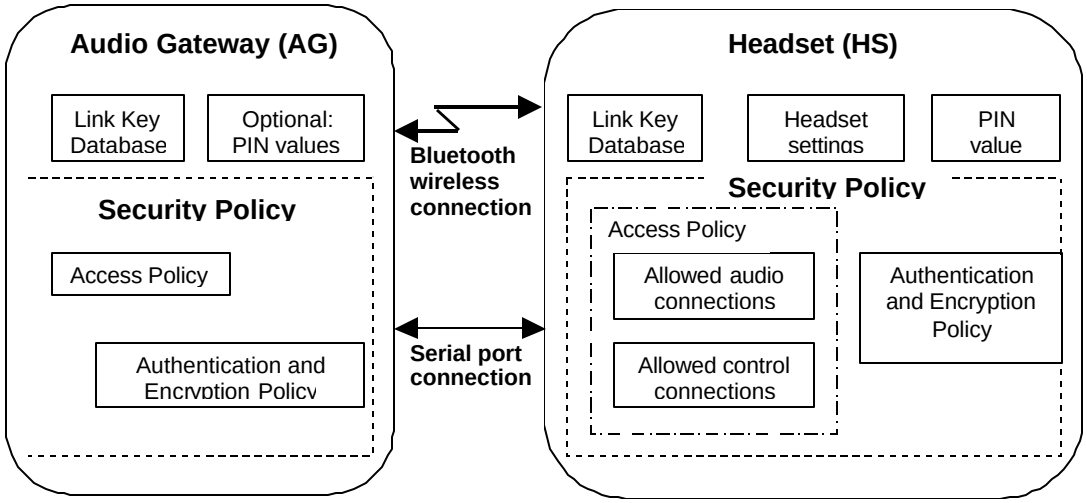

Figure 2: HS Security Architecture

The AG might use different security modes from those in the HS. It is also possible that the HS might operate in all security modes. Although Security Mode 1 provides no security, it is not excluded for an HS or AG. However, we recommend that implementers allowing an HS or AG to operate in Security Mode 1 explicitly provide a means to display that status to the user when enabled, and also provide the user with the capability to switch the device into a secure mode.

The use of Security Mode 3 for the HS is recommended. If Security Mode 3 is preset and cannot be changed by the user, Bluetooth Baseband authentication is required each time at connection set-up. This offers good protection against illegal use of a stolen HS.

3.2 Key Management

3.2.1 Bluetooth Passkey Usage and Pairing Procedure

Normally an HS does not contain an especially advanced Man Machine Interface (MMI), so inputting a new Bluetooth passkey value into the HS for each pairing might be cumbersome. Hence, a fixed Bluetooth passkey in the HS is reasonable. However, it is possible to control the settings of the HS from an external device having a better MMI, such as a PDA, a laptop, or other controller, thus allowing the Bluetooth passkey to be changed quickly and easily. Furthermore, the HS implementation should make sure that changing the Bluetooth passkey is only possible over an authenticated and encrypted Bluetooth link or a wired connection. HS manufacturers are encouraged to use randomly generated initial Bluetooth passkey values that are unique for each HS. The initial Bluetooth passkey should be stored in non-volatile memory. Higher security is provided if this memory is tamper-resistant.

If the Bluetooth passkey for a headset can be changed, it might be good practice to allow someone with physical access to the HS to reset the HS to its original (factory) Bluetooth passkey. This makes it possible for someone to continue to use their headset if they lose or forget their current Bluetooth passkey, but still have a copy of

the factory documentation that includes the initial (factory) Bluetooth passkey. With this change, the Bluetooth passkey will still give protection against theft provided that all HSs are not shipped with the same original (factory) Bluetooth passkey.

We also recommend that pairing an AG with an HS only be allowed when the user explicitly sets the HS to pairing mode. When pairing an AG with an HS, the Bluetooth passkey of the HS needs to be entered into the AG.

Since the initial exchange of keys using non-encrypted channels is the weakest part of the pairing procedure in the Bluetooth Baseband Specification [1], we also recommend that the user be in a "private area", before using the pairing procedure from the Bluetooth Baseband Specification. A "private area" is a place where you are confident that unknown devices are not in the neighborhood. Pairing in a public place, such as a point of sale, is discouraged when using the pairing procedure from the Bluetooth Baseband Specification, as there is much greater risk that a subversive unit may intercept the keys. Note that such risk only occurs if a low-entropy Bluetooth passkey value is used.

For the highest level of security when using the pairing procedure from the Bluetooth Baseband Specification, random long Bluetooth passkey values must be used. The maximum (useful) length of a passkey is 128 bits. An alternative approach for secure pairing is to provide a physical serial port interface between the AG and the HS to transfer sufficiently strong link keys directly.

3.2.2 Link Keys

The HS should use combination keys for its connections. The HS should store the combination keys in non-volatile memory. Higher security is provided if this memory is also tamper-resistant.

The AG should allow the storage of link keys in non-volatile memory. Higher security is provided if this memory is also tamper-resistant.

3.3 Connections and Control

3.3.1 Authentication and Encryption

It is feasible to use Security Mode 3 with authentication and, optionally, with encryption for the HS and AG. The AG may also use Security Mode 2 with authentication and encryption for HS connections.

3.3.2 Connection Policies

The AG and HS might use Security Modes 2 and 3, as illustrated in Figure 2, and specify different security policies for audio and control connections. However, since the HS is probably a device with simple functionality, it might prove easier to treat all connections to the HS in the same way; i.e., to use Security Mode 3 and demand authentication and encryption for all connections.

The AG might be used for several other applications. Different security policies might apply for different applications and connections. Security Mode 2 makes it possible to implement different security policies.

3.4 Example

A pairing and connection example is provided below. There are several ways of implementing HS security and HS control. Here, the use of a Bluetooth wireless connection is assumed. Also note that this example does not cover all options.

On top of the Bluetooth Baseband security, it is possible to implement additional access control mechanisms using access codes, which need to be entered each time after the Bluetooth connection between the AG and the HS has been set up. Then Bluetooth link encryption can be used to protect the transfer of the access code for verification between the AG and the HS.

Assume a new HS is delivered to a customer. The customer would like to use the HS together with his mobile phone acting as the AG. The HS is delivered with a preset Bluetooth passkey known to the customer. This passkey is intended for use in the Bluetooth LMP link key. It is assumed that HS security is implemented using preset Security Mode 3 with authentication and encryption.

The customer and the pairing units perform the following steps before the customer is able to use the HS together with the mobile phone:

- The customer sets the HS into pairing mode by pressing a button on the HS.
- The HS indicates to the user that it is ready for pairing.
- The customer prepares his mobile phone for discovery of a new Bluetooth HS device.
- The phone performs a Bluetooth inquiry and gets a response from the HS.
- As part of the LMP channel set-up, the HS demands authentication of the phone.
- The phone detects that it does not have any previous link key with the HS. Bluetooth pairing is requested.
- The phone prompts the user to enter the passkey for the HS.
- The customer inputs the passkey. A key exchange is performed between the HS and the phone. A link key is derived that is shared between the telephone and the HS.
- The new link key between the HS and the telephone is stored in non-volatile memory in both the phone and the HS unit.
- The HS authenticates the phone.
- The phone authenticates the HS.
- The HS and the phone perform an encryption key exchange.

- The LMP set-up is now complete. The HS and the phone encrypt all data they exchange from now on.
- The customer now switches the HS out of the pairing mode so it will no longer accept any new inquiries or pairing requests.

At this point, the HS will only accept connections from the telephone with which it was paired. The HS will also require authentication and encryption before any LMP channel set-up can be completed. Authentication is now based on the link key.

If the HS is stolen, the illegal user can try to set up a connection with it. This is prevented by mandatory authentication according to Security Mode 3, which is implemented in the HS in such a way that it cannot be bypassed by manually switching the phone to Security Mode 1.

If the HS owner wants to transfer the HS to another user to be used in connection with a different phone – e.g., if the owner is selling the HS – then it is recommended to change the passkey of the HS and disclose only the new passkey to the new user. It is also recommended that the existing link key in the HS be deleted.

Change of the passkey may be needed also for other purposes. Next, an example procedure is described which makes use of the existing secure Bluetooth link to change the passkey. Note, however, that if the passkey must be changed because the old passkey has been compromised, then this procedure cannot be used.

Assume now that the HS user would like to change the passkey of the HS. Then the following might take place:

- The user opens a special external device control menu on his mobile phone and asks the phone to connect to the HS.
- Using a dedicated control protocol the phone contacts the HS and establishes a control connection. In Security Mode 3 this link is the same as the one used for transferring audio stream. Note that encryption must now be enforced.
- Using a dedicated menu on the telephone the user opts to change the fixed passkey of the HS. The phone asks the user to enter the new passkey. Alternatively, a passkey handling application of the phone generates a new passkey value.
- In case of changing ownership, the new passkey is displayed on the phone, from where it is copied for the new user. Otherwise, the new passkey can be stored in the phone, in secured memory, by the passkey handling application.
- The new passkey is sent to the HS over the encrypted link.
- The HS replaces the old passkey with the new one and the old link key is deleted using the HCI command *Delete_Stored_Link_Key*.
- The old link key may also be deleted from the phone.

From now on, when the user sets the HS into pairing mode, it will only accept a pairing with the new passkey. It is advisable to store the passkey for the exceptional case that a new pairing with the HS is required; e.g., if the link key gets destroyed due to malfunction of the system. The user must keep the new passkey in a secure place. Additionally, as addressed above, it is recommended that a method to reset the passkey to the factory-installed, initial passkey be provided.

4 Dial-Up Networking Profile

This section describes security solutions and usage for the Bluetooth Dial-up Networking Profile [6].

The Bluetooth wireless technology offers authentication and encryption mechanisms on the baseband level [1] (Bluetooth Baseband Specification). They can be used to protect Bluetooth point-to-point links. The Bluetooth Baseband Security is based on the link keys that are determined for each particular Bluetooth device pair. The link key is derived during a pairing procedure. At the pairing step the Bluetooth wireless device user must either enter a Bluetooth passkey, or the same Bluetooth passkey must be available at the two Bluetooth units by some other means. This section describes how the built-in Bluetooth Baseband Security can be used for the Dial-up Networking Profile.

First the two basic dial-up networking scenarios are reviewed. Next, in Section 4.2, a sample security architecture is presented. Finally, a usage example is given.

4.1 Scope and Scenarios

Two entities are defined in the profile:

Gateway (GW): The device that provides the access to the public network. Typical devices are cellular phones and modems (see Figure 3).

Data Terminal (DT): The device that uses the dial-up service of the gateway. Typical devices are laptops and desktops (see Figure 3).

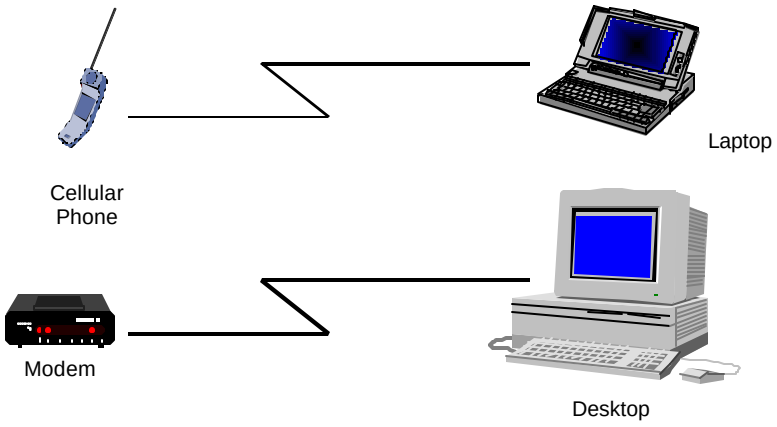

Figure 3: Dial-Up Networking Scenarios

In the Dial-Up Networking Profile [6] Bluetooth Baseband Security is required. The profile contains a basic description of the application of Bluetooth Security procedures. The purpose of this paper is to further develop that description.

4.2 Sample Architecture

4.2.1 Architecture

The Dial-up Networking Profile [6] only supports *one* connection at a time. Hence, a single DT-GW setting is considered. The profile is typically used for private modem connections. Public dial-up networking points are out of the scope of this sample architecture. A typical DT-GW configuration is shown in Figure 4.

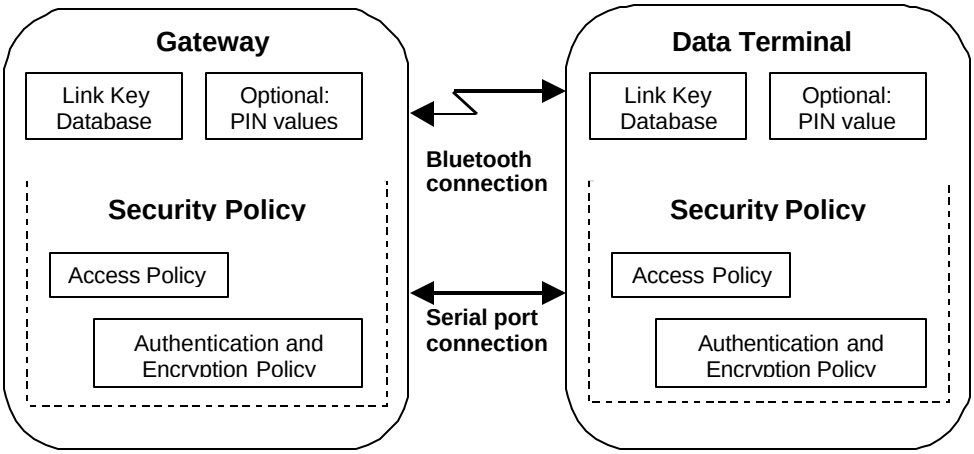

Figure 4: Dial-Up Networking Security Architecture

It is assumed that the user configures the GW and DT. Depending on the type of GW device, the user security configuration possibilities might vary. A mobile phone can have a rather advanced security policy, while a modem might have very limited configuration possibilities and hence does not allow the implementation of an advanced security policy. Typically, the modem does not have a user interface. Therefore it is appropriate to assume that an external device, such as the DT, controls some of the modem settings. Then an architecture similar to the one described for the Headset Profile applies (see Section 3.1).

It is important to provide basic protection of the Bluetooth over-the-air transmission. It is required that the air interface be as secure as the fixed LAN connection on the other side of the LAP. Hence, the Bluetooth Baseband authentication and encryption should be used to protect the link. In order to set up secure connections, the DT and GW need to store the necessary link keys.

4.2.2 Key Management

4.2.2.1 Bluetooth Passkey Usage and Pairing Procedure

The DTs do not normally use fixed Bluetooth passkey values. Depending on the type of GW device, a fixed or non-fixed Bluetooth passkey might be used. A modem

typically uses a fixed Bluetooth passkey (cf. Section 3.2.1). In the case of a fixed Bluetooth passkey, it is good practice, if possible, to frequently change its value on the GW using a control connection.

It is also recommended that it should only be possible to pair a DT with a GW when the user explicitly sets the DT and GW into pairing mode. The pairing should be performed according to the Bluetooth Baseband Specification [1]. When pairing a DT with a GW using a fixed Bluetooth passkey, the Bluetooth passkey of the GW needs to be entered into the DT. Otherwise, a new fresh Bluetooth passkey value is created by the user, and then entered to the DT and the GW. It is recommended to use an application on the DT to generate the Bluetooth passkey. Then, the generated Bluetooth passkey needs to be entered only to the GW by the user.

The user should be aware that when using the pairing procedure from the Bluetooth Baseband Specification, the initial exchange of keys using non-encrypted channels is the weakest part of the security procedure. If the pairing takes place using the pairing procedure from the Bluetooth Baseband Specification at a location where there is a risk that the communication can be eavesdropped, the GW and DT should use long random Bluetooth passkey values.

4.2.2.2 Link Keys

The use of combination keys for GW to DT dial-up connections is recommended. Unit keys are not recommended. The DT and GW should store the combination key in non-volatile memory. Higher security is provided if this memory is also tamper-resistant.

If the dial-up networking connection is a *temporary* connection, it should be possible for the user to remove the link key when the connection or session ends. The HCI command *Delete_Stored_Link_Key* can be used to remove a link key from both Bluetooth wireless modules.

A link key can be exchanged between the DT and the GW using the Bluetooth LMP link key establishment procedure. The established Bluetooth link may still be vulnerable to eavesdropping or channel hijacking if a low-entropy Bluetooth passkey is used in the link key establishment procedure.

4.2.3 Protecting Dial-Up Connections

4.2.3.1 Authentication and Encryption

The use of Security Mode 3 with authentication and encryption for the DT and GW is recommended. Security Mode 2 may also be used. If the GW is a modem, Security Mode 3 is the most appropriate for the GW. In this case, a connection is only protected over the Bluetooth link. In addition, the DT might use any of the PPP authentication mechanisms used by a network access server [23],[25],[13],[21]. If Security Mode 3 is used, all connections to the GW or DT are authenticated and encrypted. Fine grain access control in the DT can be provided at higher layers either independently or connected with the baseband authentication.

4.3 Example

The example covers pairing and connection establishment of a temporary secure connection between a DT and a mobile phone. This is only an example and does not cover all possible options.

Assume a user with a laptop borrows a mobile phone from a friend. The user would like to use the phone to get Internet access through the mobile phone using the Dial-up Networking Profile. We assume that it is possible for the user of the phone and the user of the DT to put their device into a "one-time secure connection" mode. Such a mode implies that the key derived during bonding is only used for one session and then deleted. Here a short description of the different steps at connection set-up is given:

- The phone owner switches the phone on, sets the phone into discoverable mode, and switches it into "one-time secure connection mode". This is done through a dedicated security menu.
- The DT user switches the DT into the "one-time secure connection" mode. This is done through a dedicated security menu on the DT.
- The user then asks the DT to discover neighboring Bluetooth devices (i.e., perform inquiry).
- The DT tries to set up a connection with the mobile phone. As part of the LMP channel set-up, the DT demands authentication of the phone.
- The DT and mobile phones are bonded and the user is asked to enter the same Bluetooth passkey into both devices. The user creates the Bluetooth passkey, preferably using a dedicated Bluetooth passkey generation application in the DT or in the phone.
- A pairing between the two devices is performed and a common Bluetooth combination key is calculated.
- A common link key is stored in the DT and the GW.
- Authentication is performed and the encryption key is exchanged between the devices.
- The LMP connection establishment is completed. Both the DT and the phone respectively execute the HCI command *Delete_Stored_Link_Key* with the *BD_ADDR* of the phone and the DT.
- A serial port emulation connection is established between the DT and the phone.
- The DT uses AT commands to set up the desired dial-up connection.
- Dial-up data can securely flow between the DT and the phone.
- When the call is finished, the Bluetooth wireless connection is released. The recently derived encryption keys in the DT and phone Bluetooth modules are deleted.

5 LAN Access Profile

In this section we describe sample security architectures for the Bluetooth LAN Access Profile [7]. We use the LAN Access Profile as a reference model. However, the SIG is about to release a new PAN Profile that will replace the LAN Access Profile. The architecture we describe here can be applied also to the new PAN Profile [10].

The section is divided into two parts. The first part describes an architecture based on built-in security mechanisms. The second part describes an architecture for an access point roaming scenario. This part introduces a new key concept, so-called *group keys*. Section 5.2 is included in order to illustrate how the Bluetooth link security complemented with network security functions can be used also for rather complex public access scenarios.

5.1 Using the Built-In Security Mechanisms

The Bluetooth wireless technology offers both authentication and encryption at the baseband level [1] (Bluetooth Baseband Specification). These mechanisms can be used to protect connections to both personal and non-personal devices. LAN access is one example where one Bluetooth wireless device might be connected to several different types of devices. In this section we show how the Bluetooth Baseband Security mechanisms can be utilized to secure communication for LAN access for the scenarios covered by this profile [7].

The section is organized as follows. First, the scenarios covered by the profile are described. Next, in Section 5.1.2, different communication security options are discussed. Finally, in Section 5.1.3, a sample security architecture is provided.

5.1.1 Scope and Scenarios

There are two different roles defined in the profile [7]: the LAN Access Point (LAP) and the Data Terminal (DT). The LAP is the Bluetooth wireless device that provides access to the LAN (e.g., Ethernet, Token Ring, Fiber Channel, Cable Modem, Firewire, USB, Home Networking). The DT uses the services of the LAP. Typical devices acting as data terminals are laptops, notebooks, desktops PCs, and PDAs.

The following scenarios are described in the LAN Access Profile:

1. A single DT uses a LAP as a wireless means for connecting to a LAN.
2. Multiple DTs use a LAP as a wireless means for connecting to a LAN.
3. PC-to-PC connection where two Bluetooth wireless devices can form a single connection with each other. The three different scenarios are shown in the figures below.

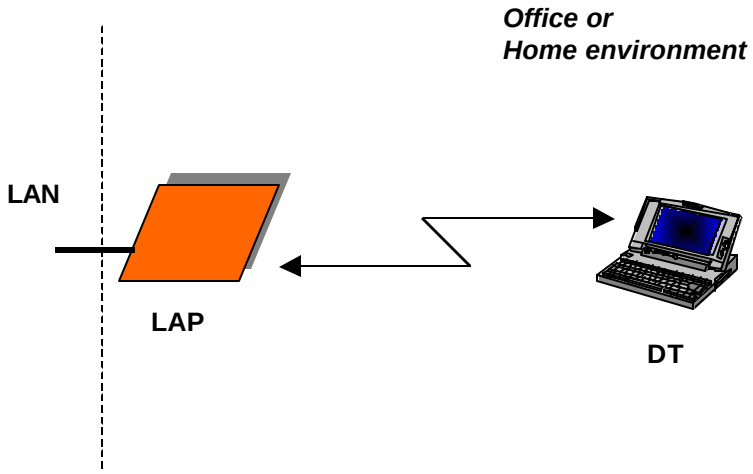

Figure 5: A Single DT uses a LAP

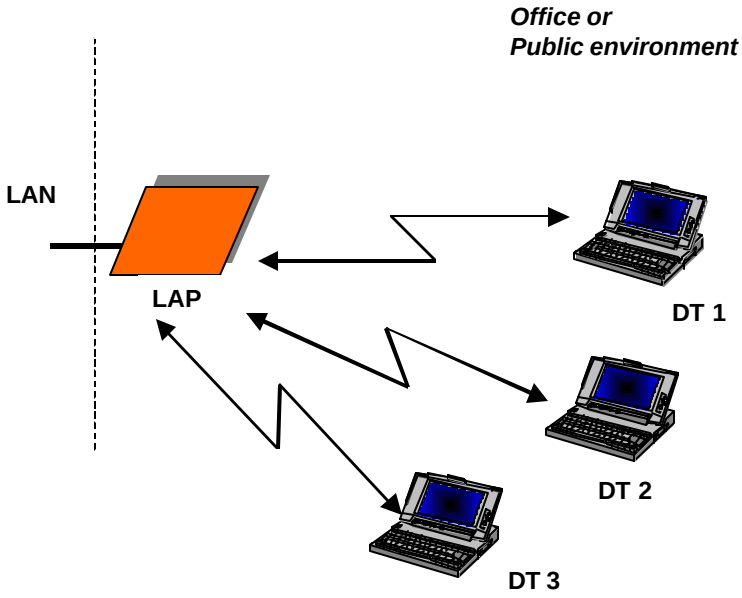

Figure 6: Multiple DTs use a LAP

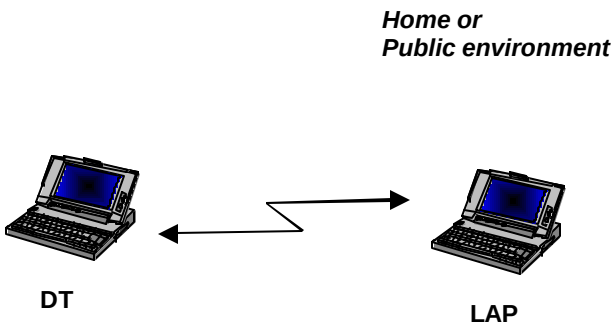

Figure 7: PC-to-PC Connection

5.1.2 Communication Security, at Which Layer?

For a communication service, several different security aspects must be taken into account. These aspects cover everything from protection of communication links (provided by encryption and/or data integrity protection), authentication of devices or users, and access control. Different security mechanisms can be applied at different layers in the communication stacks. Furthermore, protection at one layer does not exclude protection at another level. The security demands depend on the application, the environment, and usage scenario. For one usage scenario, basic authentication of devices might be a sufficient security level, while for yet another, link-level encryption, link-level authentication, *and* authentication and authorization at the application level are needed. In Figure 8, the LAN access protocol stack is shown. Different security mechanisms at different protocol levels are indicated.

This paper concentrates on describing solutions based on the Bluetooth Baseband Security. However, PPP and IP security protection mechanisms are also described. Although important, application-level security mechanisms are outside the scope of this paper.

The Bluetooth Baseband provides authentication and encryption. How and when these mechanisms should be used is determined by policy rules. In Section 5.1.3, different possible security policies are discussed.

The LAN Access Profile depends on both the Serial Port Profile and the Generic Access Profile. The Serial Port Profile provides RS-232 serial cable emulation for Bluetooth wireless devices. The Generic Access Profile (GAP) [1] describes several security aspects of Bluetooth wireless connections. Since the LAN Access Profile inherits characteristics from the GAP, these aspects also apply to the LAN Access Profile.

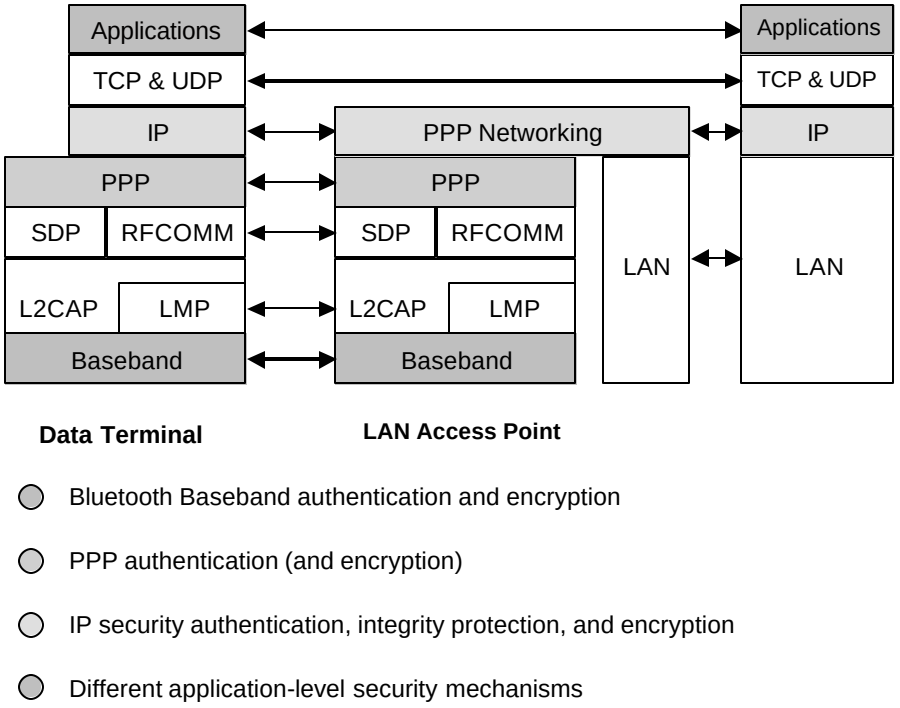

Figure 8: LAN Access Protocol Stack and Security Protocol Options

The usage of the different security modes for the different scenarios is described in Section 5.1.3.

5.1.3 Sample Architecture

The architecture we present here can be used for all three LAN access scenarios. We assume the use of the built-in security to manually pair the DT and LAP. Manual pairing is suitable to use when a user uses one particular LAP for a long time period (at least several days). Even if possible, it would be cumbersome for the user to enter a new Bluetooth passkey value each time he or she would like to connect to a particular LAP. Manual pairing is also well suited for Scenario 3 situations.

Authentication and encryption can be provided on IP or application level. For example, IPsec [19] with IKE [15] can be used at the IP (or more precisely at the UDP) level. A protocol like IPsec is most suitable to secure *end-to-end* IP services like Virtual Private Network (VPN) services. IPsec can be used for any IP connection independent of the particular access method. Here only LAN access using the Bluetooth wireless technology is considered and IPsec configurations are not described. It is important to notice that the use of link-level security and VPN solutions do not exclude each other, but rather complement each other.

A large number of different application-level authentication and encryption mechanisms exist. This can be anything from secure Web and email to different e-commerce services. These applications are independent of the access method and outside the scope of our sample architecture.

5.1.3.1 Architecture

We assume the LAP to be *physically* located at a place where unauthorized users cannot manipulate it or that the LAP has some built-in security mechanisms that prevent unauthorized access to it. A typical DT-LAP (Scenario 1 or 2) configuration is shown in Figure 9. Similarly, a typical DT-DT (Scenario 3) configuration is shown in Figure 10.

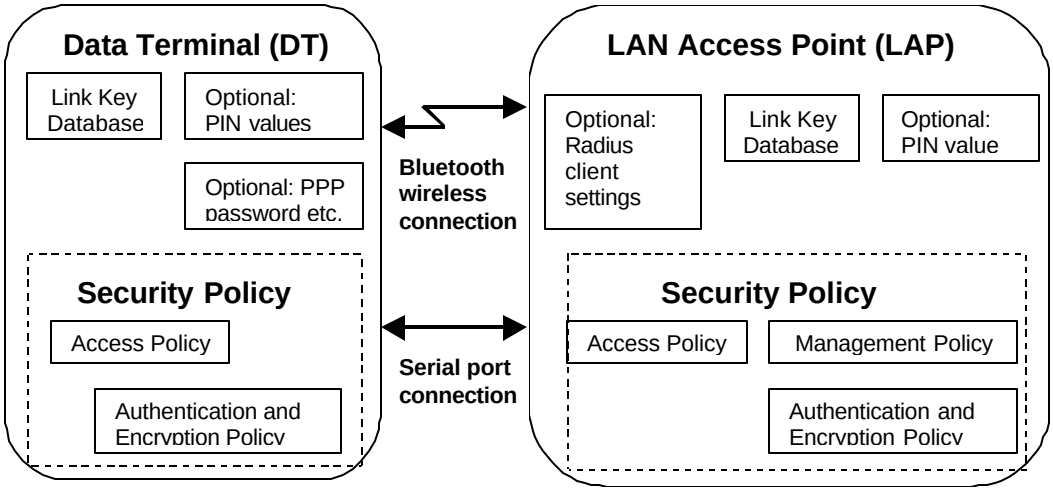

Figure 9: Security Architecture for the DT-LAP Scenario

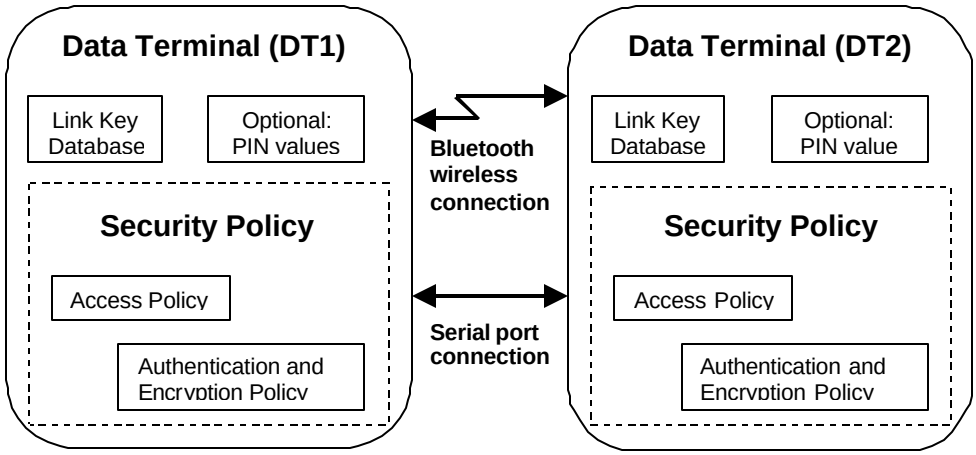

Figure 10: Security Architecture for the DT-DT Scenario

It is important to provide basic protection of the Bluetooth air transmission. It is required that the air interface is as secure as the fixed LAN connection on the other side of the LAP. Hence, the Bluetooth Baseband authentication and encryption can preferably protect the link. In order to set up secure connections, the LAP and DT need to store necessary keys. Bluetooth link keys are suitable for this purpose.

It is assumed that the LAP can be managed by a user interface or through network management. It is important to ensure that only authorized users are allowed to change the setting and especially the security settings of the LAP. Hence, access

control should be implemented on the LAP. For example, a user can be forced to enter a particular access code before he or she is allowed to perform any management functions on the LAP. The LAP might also be managed remotely. Secure remote node management is a large area with several different possible solutions. The preferred solution depends very much on the structure of the LAN. For example, SNMPv3 [16], [20], [12] includes possibilities for secure remote node management.

It is assumed in this security architecture that all DTs have appropriate user interfaces that can be used to set up the security configuration and needed policy settings.

The LAN Access Profile is defined over PPP. PPP supports a number of different authentication and encryption protocols [23], [25], [13], [21]. These security protocols can be used in addition to the protection provided by the baseband. For example, PPP authentication might be required to authenticate DT users.

5.1.3.2 Key Management

Bluetooth Passkey Usage and Pairing Procedure

Here we describe pairing based on the built-in pairing mechanism. The user should be aware of the fact that the initial exchange of keys based on the built-in Bluetooth pairing mechanism is the weakest part of the Bluetooth link-level security. Using short passkey values is a potential security risk as described in Section 1. If the pairing takes place at a location where there is a risk that the communication is eavesdropped, the LAP and DT should use long random Bluetooth passkeys. Alternative higher-layer key exchange options such as Diffie-Hellman key exchange can be used to derive a strong long PIN [1].

The DTs do not normally use fixed Bluetooth passkey values. LAPs might use a fixed Bluetooth passkey. In the case of a fixed Bluetooth passkey, it should be possible to frequently change the fixed Bluetooth passkey of the LAP. Depending on the management system of the LAP this can be done in several different ways. If the LAP contains a user interface, that interface can provide the possibility for an authorized manager to change the Bluetooth passkey setting of the LAP. The LAP might also be managed remotely over a network connection. Secure remote management (see above) is not discussed here. However, independent of whether the LAP is managed locally or remotely, before changing the fixed Bluetooth passkey the LAP manager should be authenticated by some secure authentication mechanism.

If the user is allowed to get management access to the LAP, the LAP can use a non-fixed Bluetooth passkey. If it is possible for anybody with a DT to make a pairing with the LAP, the access to the LAP should be *physically* restricted. This could be the case in a home or small office environment. If the LAP is located in a public environment and uses a non-fixed Bluetooth passkey, there should be restriction of who is allowed to make the manual pairing with the LAP. Restricted access can be

provided by a particular access code that the user needs to enter into the LAP before it is set into “pairing mode”.

Link keys

The LAP might use a unit key or a combination key for its connections. The use of unit keys is not recommended. Both the DTs and LAPs should use combination keys. The DT and LAP should store the combination key in non-volatile memory. Higher security is provided if this memory is also tamper-resistant.

If the manual pairing is used for setting up a *temporary* connection, it should be possible for the user to choose removal of the link key when the connection or session ends. This is especially important for Scenario 3 situations. The HCI command *Delete_Stored_Link_Key* [2] can be used to remove a link key from a module.

5.1.3.3 Protecting PPP Connections

Authentication and Encryption

The use of Security Mode 3 or 2 with authentication and encryption always switched on in the DT and LAP is recommended. In this case the connection is only protected over the Bluetooth link. In addition to this, the LAP might use any of the PPP authentication mechanisms. However, for single DT-LAP scenarios there is no direct need for an additional PPP authentication mechanism.

Access Policies

If Security Mode 3 is used, all connection towards the LAP or DT is authenticated and encrypted. Access control can be provided at higher layers independently or connected to the Baseband authentication.

If Security Mode 2 is used, no security procedures are initiated before a channel establishment request has been received. Access control might be provided according to [11] (Security Architecture White Paper). The architecture in [11] uses a security manager. Alternative implementations are also possible. The access control implementation is host-specific and should not cause interoperability problems. The access policy will very much depend on the particular DT and LAP. We do not give any general policy recommendations.

5.2 Access Point Roaming

Now we extend Scenario 2 and consider a situation where a DT is roaming between several different LAPs belonging to the same LAN. The DT might connect to both previously visited LAPs and LAPs to which it has never previously connected. The connection might, for example, be Internet access at a hot spot area. The static security relationships between the DT and LAP that we assumed in Section 5.1 do not work well for this new scenario. Consequently an alternative security architecture is described below.

The section is structured as follows. First we describe a slightly new key concept for Bluetooth wireless technology, so-called group keys. The security architecture is based on the usage of group keys. In Section 5.2.2 we give an overview of the architecture. Section 5.2.3 describes key management. Finally, in Section 5.2.4 we give our recommendations on how to protect the PPP LAN access connections while roaming.

5.2.1 Group Keys

We build our security architecture on a slightly new key concept. We introduce so-called *group keys*. Currently, there are two main types of link keys defined in Bluetooth wireless technology: *combination keys* and *unit keys*. Unit keys have some security drawbacks and we do not recommend their use.

A combination key is unique for each combination of Bluetooth wireless units. For the scenario we are considering we have one DT that we would like to connect to many different LAPs. It would be very cumbersome to demand that all the different distributed LAPs share a combination key with any DT that has subscribed to the service. Hence, it is not feasible to use a combination key. Furthermore, the current Bluetooth Specification only describes how to create link keys when pairing two devices. It is not reasonable to assume that the user should pair his device with all possible LAPs of the service provider.

With very small changes, we can use the built-in Bluetooth Security mechanism for the access point roaming. The new idea is that we assume that a link key is not unique for one *link* but is used by one unit for one particular *service.* This type of new link key is called *group key.* We assume that before a unit subscribes to a new service, a *group key* for that particular service is generated. Later, when the user of the unit would like to utilize the service, the keys are obtained from the service ID using the SDP and make a lookup in the internal key database. It might be possible for the user to enforce his unit to only use ordinary combination keys for some connections while it still might allow *group key*s for other types of connections. For example, the key memory in the host might be like the example in Table 1 below.

Service	BD_ADDR	Usage	Key
LAN access A		Service-dependent	AB124223 23E23A12 1264BEF1 A2845D28B
LAN access B		Service-dependent	2343AF23 A68BEA396 9464B47E6 496ECA
Any	3FA12437BC45	Always	23BD378A 93678928 AB2784BD FE376925
Any	D234BD6A24E9	Always	374585937 2691A373 12FD2839 CF381749

Table 1: Example of a Group Key Database, One Key in Each Row

In the table, records for combination keys have the *BD_ADDR* field filled with the corresponding Bluetooth device address (*BD_ADDR*). The group keys have an empty *BD_ADDR* field. In the example, the two first keys are group keys while the two second are combination keys.

The current Bluetooth Specification does not use the group key concept or any group key database. However, group key usage can be implemented (using Security Mode 2) by having the link key database implemented in the host instead of in the Bluetooth wireless module. The host and not the module then take care of all key handling; i.e., storing, updating, deleting keys, etc. The host should store the keys in non-volatile memory. Preferably, this memory is also tamper-resistant. The HCI commands [2]: *Read_Stored_Link_Key*, *Write_Stored_Link_Key*, and *Delete_Stored_Link_Key* can be used to pass key information between the host and the module.

5.2.2 Architecture

We are considering a situation where a DT can move around and access several different LAPs belonging to the same LAN access service provider. In order to be user-friendly, manual configuration by the user at each new connection set-up should be avoided.

One general possible security principle for the architecture would be to use totally open (from the security point of view) LAPs that can be accessed by anybody. But, often the LAP service provider would like to restrict the access to the LAP. Furthermore, the DT user would like to be sure that he connects to the correct LAP and that the traffic sent over the Bluetooth radio interface is not eavesdropped. Hence, we describe an architecture where the Bluetooth Baseband authentication and encryption is used to protect the access link. We recommend Bluetooth Baseband authentication to control that only legitimate users are able to connect to the LAN.

We distinguish between two different situations (from the DT point of view):

1. **Establish initial trust relation**: At the initial connection between DT and LAP group link keys are exchanged. This is analogous to Bluetooth pairing except that the resulting link key is shared among the LAPs providing the service.
2. **Subsequent access to LAPs**: Here we utilize the group unit concept to allow fast convenient access to different LAPs.

In order to obtain a high security level, the LAP should either be *physically* protected so that unauthorized users cannot manipulate it, or have some built-in security mechanisms that prevent unauthorized access to it. The LAP can be managed by a user interface or through network management (see also Section 5.1.3.1).

We assume that all DTs have appropriate user interfaces that can be used to set up the security configuration and policy setting needed.

The LAN Access Profile is defined over PPP. PPP supports a number of different authentication and encryption protocols [23], [25], [13], [21]. These can be used in addition to the protection provided by the baseband. PPP authentication and encryption is discussed in the two subsequent subsections.

We assume that a DT is able to get information (through SDP) of the LAN access service before trying to set up a PPP connection. Hence, Security Mode 2 must be used.

5.2.3 Key Management

Next we describe how the necessary group key is obtained; i.e., how to create the necessary initial trust relation. Two options on how to obtain the group key are shown. The first option is based on Bluetooth passkeys and the second on any other secure relationship between the DT user and the LAN access provider. This could be any suitable security method like a trust relation based on certificates.

5.2.3.1 Initial Trust Based on Bluetooth Passkeys

Assume a user would like to register his DT for getting LAN access through LAPs installed by a certain LAN access service provider or organization. A user who registers the DT at the LAN access provider might do this using a non-Bluetooth wireless procedure (phone, office, Web, etc.).

For this option we assume that when a DT user subscribes to a LAN access service it gets a unique ID that identifies the service provider. Together with the ID the user also receives a secret Bluetooth passkey. The passkey is used to perform Bluetooth bonding. In order to provide high security for the system, a long passkey value must be used. The Bluetooth passkey is generated by the LAN access service provider using a secure random generator and is unique for each DT subscriber in the LAN. The DT user (or someone on behalf of the DT user) needs to manually enter into a well-protected LAN access service database the two values:

- LAN access service ID
- Bluetooth passkey for the particular LAN access service

Also at the registration the user is given a unique DT ID to the LAN access provider. This ID can be LAN access-specific or it can be the DT Bluetooth wireless device address.

As part of the subscription, the LAN access provider stores the Bluetooth passkey and corresponding DT ID (which might be the Bluetooth wireless device address) in a central secure database. All LAPs in the access network need to have secure access to this database as described in Figure 11.

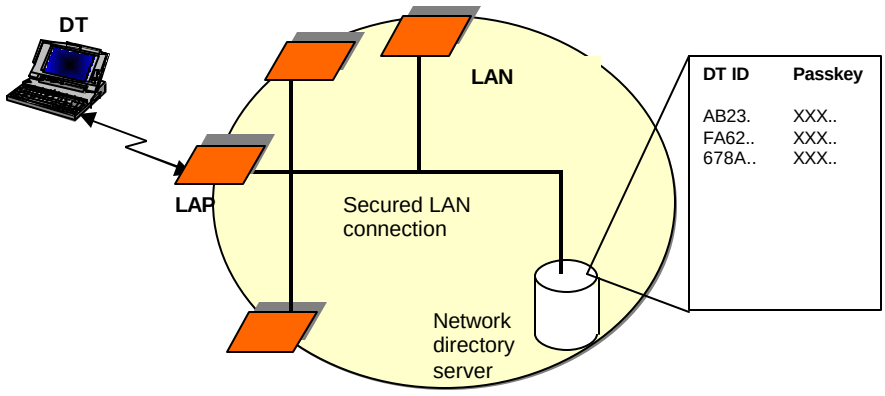

Figure 11: LAN Access Network Architecture with Subscription Server Containing User's Bluetooth Passkeys

The access to the database can be secured by, for example, TLS [14]. The initial connection might be performed according to Figure 12.

Below we give a detailed description of each step in the pairing procedure:

1. The DT connects to the LAP or the LAP connects to the DT using the ordinary paging procedure [1].
2. The DT acts as an SDP client and searches for a LAN access service record on the LAP. The DT receives the service ID of the LAP. We do not describe the exact format of the SDP needed records. The LAP may perform a similar service discovery sequence on the DT to obtain the DT ID. However, if the DT ID is the device address of the DT this is not necessary.
3. The DT checks that it knows the service ID received over the SDP protocol. Otherwise, the DT interrupts the connection procedure.
4. The DT asks the internal service database for the Bluetooth passkey corresponding to the service ID.
5. The LAP makes a secure network connection towards the network directory server to obtain the Bluetooth passkey corresponding to the received DT ID.
6. The DT and LAP perform Bluetooth bonding using the Bluetooth passkey obtained from the databases. As a result of the bonding, the DT and LAP share a common link key.

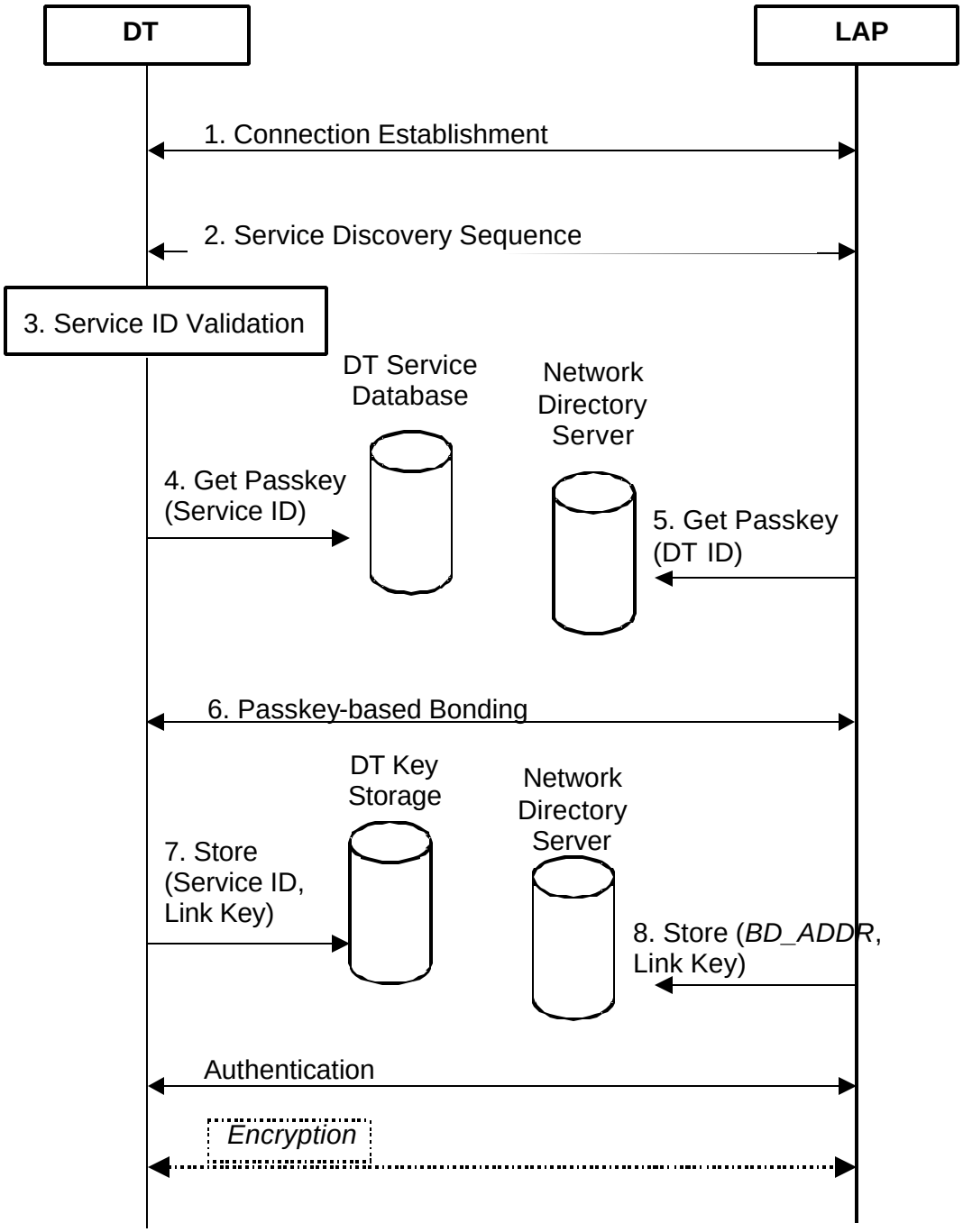

Figure 12: Initial Pairing Procedure

7. The DT uses the HCI command *Write_Stored_Link_Key* to store the derived key in the Bluetooth wireless module. The key is also stored as a group key for the LAP service in the key database of the host.
8. The LAP uses the HCI command *Write_Stored_Link_Key* to store the derived key in the Bluetooth wireless module. The key is also stored as a group key for the DT in the network directory server. The key might be identified by the *BD_ADDR* of the DT.

5.2.3.2 Initial Trust Based on Any Authenticated Key Exchange Mechanism

As an alternative to the Bluetooth passkey-based initial trust establishment described in Section 5.2.3.1, we can use any key exchange mechanism to derive the group key. This can, for example, be a public key-based or shared key-based method. Any standard method like TLS [14] or SRP [24] together with TLS is recommended. In Figure 13 we show the message flow for this option.

Below we give a detailed description of each step in the pairing procedure:

1. The DT connects to the LAP or the LAP connects to the DT using the ordinary paging procedure [1].
2. The DT acts as an SDP client and searches for the LAN access service record on the LAP. The DT receives the service ID of the LAP. We do not describe the exact format of the SDP needed records. The LAP may perform a similar service discovery sequence on the DT to obtain the DT ID. However, this is not necessary if the DT ID is the device address of the DT.
3. The DT checks that it knows the service ID received over the SDP protocol. Otherwise, the DT interrupts the connection procedure.
4. A higher-layer authentication and key exchange is performed. As a result of the key exchange, the DT and LAP share a common strong link key.
5. The DT uses the HCI command *Write_Stored_Link_Key* to store the obtained link key in the Bluetooth wireless module. The key is also stored as a group key for the LAP service in the key database of the host.
6. The LAP uses the HCI command *Write_Stored_Link_Key* to store the derived link key in the Bluetooth wireless module. This key is also stored as a group key for the DT in the network directory server. The key might be identified by the *BD_ADDR* of the DT.

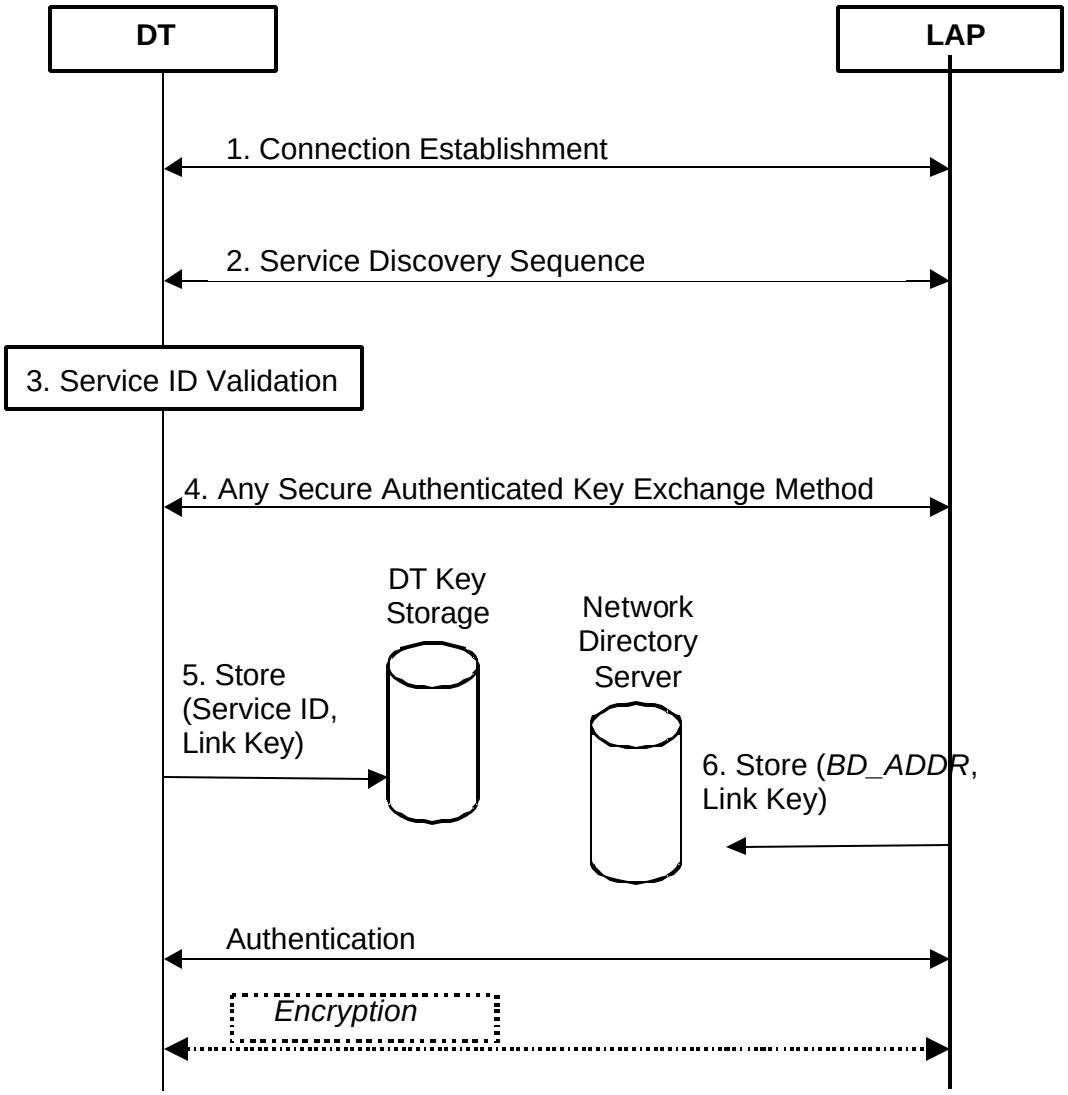

Figure 13: Initial Connection and Authentication Procedure

5.2.3.3 PPP Passwords or Keys

In addition to the Bluetooth keys, the LAN access service provider might use PPP passwords or keys to authenticate the DT user. The storing and retrieving of the PPP username, password, and keys can be manually configured into the DT host according to current standard methods; i.e., manually enter username and password into the host. When using PPP authentication there must be an infrastructure taking care of LAP users and subscriptions. One common way is to use a RADIUS client [22] at the LAP connecting to a RADIUS server [22], which has access to a subscription database. A typical configuration is shown in Figure 14 below.

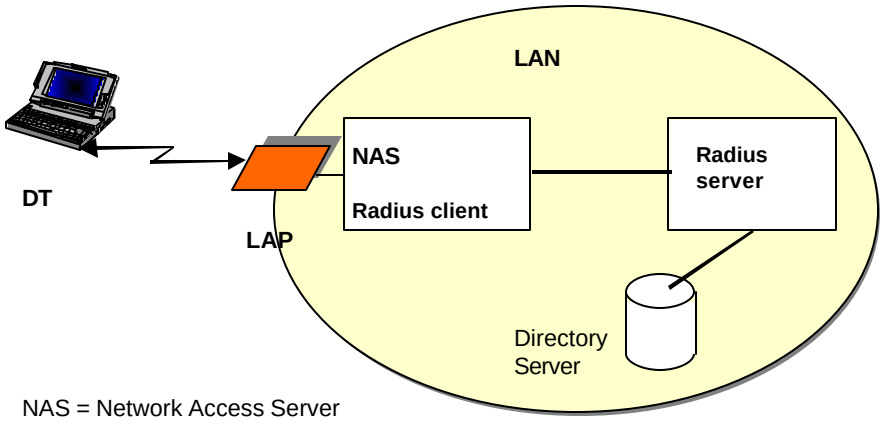

Figure 14: LAN Access Network Architecture with Radius Server

5.2.4 Protecting PPP Connections; Subsequent Access to LAPs

5.2.4.1 Authentication and Encryption

We assume the usage of Security Mode 2. This means that no security procedures are initiated before a channel establishment request has been received or a channel establishment procedure has been initiated. We assume the group key concept that we described in Section 5.2.1. The group key concept can only be used together with Security Mode 2. If the DT connects to the LAN for the fist time, authentication and encryption are performed according to the description in Section 5.2.3. For all other cases, the procedure is as described in Figure 15.

Below we give a detailed description of each step in the secure connection establishment:

1. The DT connects to the LAP or the LAP connects to the DT using the Bluetooth paging procedure [1].
2. The DT acts as an SDP client and searches for the LAN access service record on the LAP. The DT receives the service ID of the LAP. We do not describe the exact format of the SDP needed records.
3. The DT checks that it knows the service ID received over the SDP protocol. Otherwise, the DT interrupts the connection procedure.
4. If this is not the first time the DT connects to this particular LAN, the DT reads the group key corresponding to the received service ID from the DT key storage.
5. The LAP makes a secure network connection towards the network directory server to obtain the link key corresponding to the *BD_ADDR* of the connected DT. As an alternative to the *BD_ADDR*, the LAP can use any other identity obtained during the service discovery sequence.
6. The DT and LAP use the HCI command *Write_Stored_Link_Key* to make the link key available to the respective Bluetooth wireless modules. Mutual authentication is then performed according to [1] (Bluetooth Baseband Specification).

The link is encrypted according to [1].

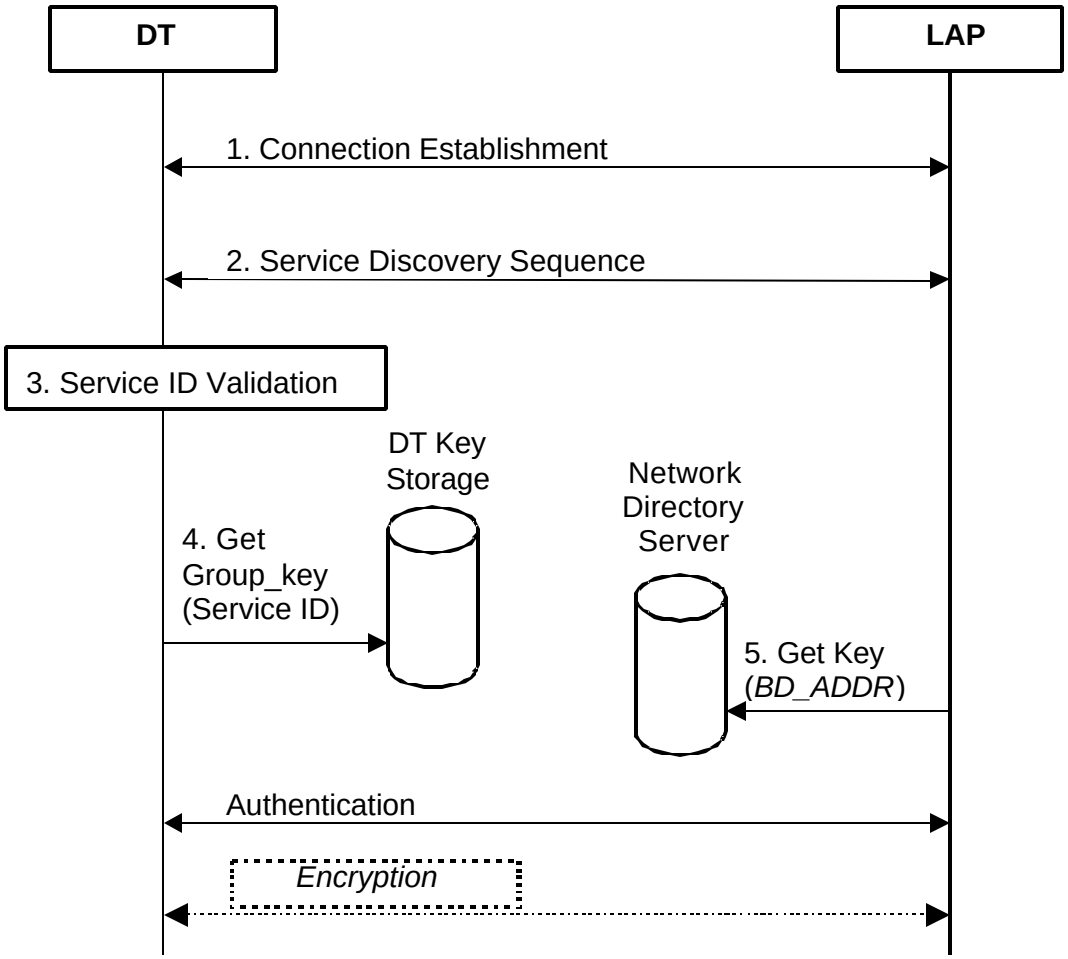

Figure 15: Connection Procedure with Baseband Authentication and Encryption

In addition to the Bluetooth Baseband authentication, the access network might demand a PPP authentication [23], [25], [13]. Optionally, the network might also demand PPP encryption [21]. We do not give any detailed description of PPP authentication or encryption.

5.2.4.2 Access Policies

Access control might be provided according to [11]. This demands that a security manager is implemented as described in [11]. Alternative implementations are possible. The access control implementation is host-specific and should not cause interoperability problems. The access policy will very much depend on the particular DT and LAP and we do not give any general policy recommendations.

6 Synchronization Profile

This section describes security solutions and usage models for the Bluetooth Synchronization Profile [9]. The Synchronization Profile defines requirements, protocols, and procedures to be used for applications that implement this usage model. Currently, the profile enables four application classes: phone book, calendar, messaging, and notes.

The profile itself does not give recommendations regarding important security issues to be considered for this model. The synchronization service involves operations on PIM (Personal Information Management) data. Frequently, this data is highly confidential. No matter whether the PIM data is private or business-related, it is very important to protect this service against any misuse. Therefore, a security architecture is suggested to protect against passive or active attacks, which could exploit weaknesses in the implementation of the Synchronization Profile. The objective is to deny an unauthorized party the ability to disclose, destroy, or alter information.

Here the analysis is restricted to an attacker who does not have physical access to the device he tries to compromise. Recommendations on methods to protect stored information on the diverse set of devices used in these scenarios are outside the scope of this paper.

6.1 Scope and Scenarios

This profile (see Figure 16) uses OBEX over RFCOMM. OBEX [8], in this context, is the Bluetooth adaptation of IrOBEX [17]. Synchronization is made using a client-server model that is compliant to the Telecom/IrMC Synchronization Service defined in the IrMC Specification [18].

From Figure 1, it follows that this profile must comply with the requirements in the Generic Object Exchange [8], Serial Port, and Generic Access [1] Profiles. The profile stack that is common for all usage models dependent on the Generic Object Exchange Profile is shown below.

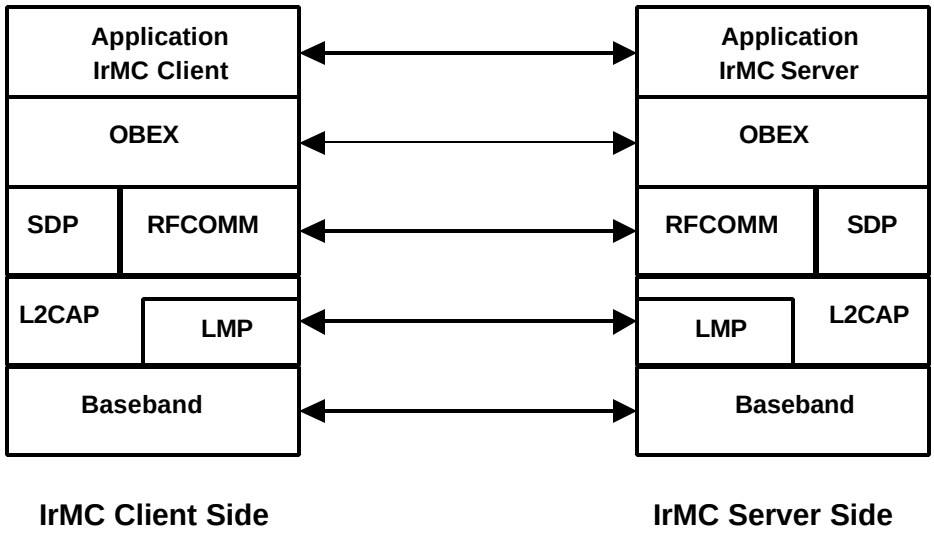

Figure 16: Synchronization Protocol Stack

The IrMC client, containing the Sync engine, will initiate an OBEX session with the IrMC server that contains the object exchange server. The IrMC client uses OBEX PUT and GET requests to push and pull PIM data to and from the IrMC server. Typically, the client resides in a laptop or PC, and the server in a PDA or mobile phone.

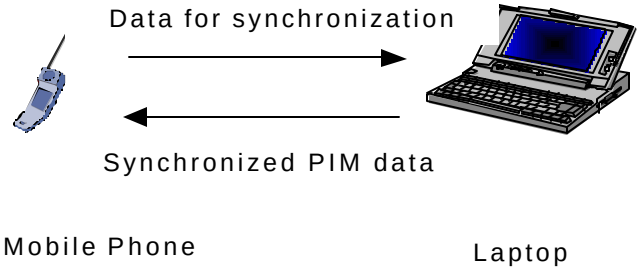

Figure 17: Synchronization between Phone (IrMC Server) and Laptop (IrMC Client)

The following user scenarios are covered:

1. The user manually initiates synchronization on the IrMC client device.
2. The user manually initiates synchronization on the IrMC server device.
3. Synchronization is performed automatically; i.e., without user intervention, initialized (initiated?) by the IrMC client.

The second scenario covers the case where a user of a mobile phone pushes a “Sync” button to request the Sync engine on a PC to begin synchronization. Here the phone must first act as an IrMC client and request the PC to begin synchronization.

The PC must receive this request as an IrMC server, and then initiate a new connection as an IrMC client to synchronize with the IrMC server in the phone.

6.2 Security Model

6.2.1 General Architecture

This profile (see Figure 16) allows security mechanisms at baseband, OBEX, IrMC client/server, and UI level. At baseband we have the usual Bluetooth authentication and encryption, mandated by the Synchronization Profile [9]. The IrOBEX Specification [17] includes an authentication mechanism, the support of which is mandated in [9]. On the user interface level, authorization for access security can be used. The use of other security mechanisms is discouraged since they are not needed.

6.2.1.1 OBEX Authentication and Sessions

The OBEX authentication is a challenge/response scheme based on the MD5 cryptographic hash function that may be used to get an authenticated OBEX session. It depends on an initialization procedure in which a common password must be entered and stored in both devices. If OBEX authentication is to be used, the initialization must occur before the first OBEX connection is established. Furthermore, if OBEX authentication is used, the Generic Object Exchange Profile [8] requires that OBEX sessions without OBEX authentication must be supported. This can, for example, be an application of the Business Card Exchange feature in the Object Push Profile. The latter makes use of the OBEX Inbox Service available via an OBEX session initiated by a CONNECT request without a Target header; see the PAN Profile [10] for more information.

For the synchronization service, establishment of an OBEX session *must* start with the IrMC client making a CONNECT request using the target header with value *IRMC-SYNC*. The OBEX server then redirects this request to the IrMC server. If OBEX authentication is to be used, the IrMC server initiates this (mutual) authentication that is performed before the connection is established. In this way, we can make use of the OBEX authentication without any conflict to other applications using the OBEX default server without authentication.

6.2.2 Sample Architectures

Here, two variants are described. Both of them use Bluetooth authentication and encryption to protect the link. The first variant uses authorization for access security, while the second makes use of OBEX authentication to prevent unauthorized usage of the synchronization service.

It is likely that the devices involved in the synchronization support several Bluetooth applications with varying security requirements. The use of Security Mode 2 (see [1]) is therefore suggested for both sample architectures given below.

6.2.2.1 Sample Architecture using Authorization

The IrMC server and client shall be paired before the first synchronization. Bluetooth Baseband authentication and encryption, which is suitable to protect the link from eavesdropping of the synchronization messages, shall be used. It is further suggested that a database of trusted (and paired) devices be used, both on the server and client side.

Access to the synchronization service shall be automatically granted to trusted devices. For untrusted devices, authorization on the IrMC server device is required. For Scenarios 1 and 3, this is typically the mobile phone, but for Scenario 2 this is typically the PC, when it receives the Sync command from the phone. The described access policy can be implemented as described in [11], although it doesn't have to be that general.

A scenario where a user accepts pairing of his device (e.g., his phone) with another device in order to take advantage of some service provided via that device, shows the need for authorization. In this case it would be unwise to (implicitly) allow the other device access to the synchronization service, by acting as an IrMC client. The requirement of authorization will prevent this if it is not wanted, while keeping flexibility to allow this in a controlled manner if this is indeed the intention of the user.

6.2.2.2 Sample Architecture using OBEX Authentication

Here it is also required that the IrMC server and client be paired before the first synchronization, and that Bluetooth Baseband authentication and encryption be used. This will prevent an eavesdropper from gaining access to information from the synchronized object store. To prevent an active attacker from taking the role of an IrMC client or server and gaining access to the synchronization service, the use of OBEX authentication is suggested (see Section 6.2.1.1). This solution is less flexible than the previously described model based on authorization, but can provide a higher degree of security, depending on the quality of key management (see Section 6.2.3).

For implementers, we stress again the requirement from the Generic Object Exchange Profile [8] that the synchronization service must use an OBEX session initiated with a CONNECT request with target header value *IRMC-SYNC*. It will then receive a connection identifier to be used in subsequent GET and PUT requests. GET requests with the NAME header starting with *telecom/* will be redirected to the IrMC server. But if the request does not have a valid connection identifier, the IrMC server must not accept it.

6.2.3 Bluetooth Passkeys and OBEX Passwords

It is strongly recommended that combination keys be used for this profile. To achieve a high level of security, care has to be taken at the time of pairing the devices, and also when performing the OBEX initialization if OBEX authentication is to be used.

If short or non-random Bluetooth passkeys are used, and if it is possible that the exchanged messages have been eavesdropped during the pairing, it is possible that

the derived link key has been compromised. Therefore, it is recommended that either the pairing shall take place in a "private area" or long random Bluetooth passkeys shall be used. A "private area" is a place where you are confident that unknown devices are not in the neighborhood.

A strong confidentiality protection of the link is important to prevent eavesdropping of synchronization messages. But it is also important to protect the connection identifier of the OBEX session, and the OBEX authentication challenge/response messages. If weak OBEX passwords are used and if the Bluetooth link keys have been compromised, then the overall security will be compromised. For this reason it is also required that OBEX passwords be long and chosen randomly, independent from the Bluetooth passkey.

6.3 An Initial Synchronization Example

Here is an example on the UI level, showing the initial synchronization according to Scenario 1. The first sample architecture described above may be performed.

Step	IrMC Client	IrMC Server
1	The user performs bonding of the devices. He may register the server device in the trusted devices DB of the client device, and *vice versa*.	
2		The IrMC server must be in connectable mode. If not, the user must activate this mode on the device.
3	The user activates an application for synchronization.	
4	A list of devices in the RF proximity of the IrMC client is displayed to the user.	
5	The user selects a device to be connected and synchronized.	
6	The user is alerted if the device does not support the synchronization feature, and the user may select another device.	
7		If the IrMC client device is untrusted, the user is alerted that synchronization will be performed. By some device-specific interaction, the user accepts this.
8	The first synchronization is processed.	
9	The user may be notified of the result of the operation.	

Table 2: An Initial Synchronization Example for the Architecture Using Authorization

7 References

[1] Bluetooth SIG, Specification of the Bluetooth System, Core
Part B: Baseband Specification
Version 1.1, 22 February 2001, http://www.bluetooth.com/

[2] Bluetooth SIG, Specification of the Bluetooth System, Core
Part H-1: Host Controller Interface Functional Specification
Version 1.1, 22 February 2001, http://www.bluetooth.com/

[3] Bluetooth SIG, Specification of the Bluetooth System, Profiles
Part K-1: Generic Access Profile
Version 1.1, 22 February 2001, http://www.bluetooth.com/

[4] Bluetooth SIG, Specification of the Bluetooth System, Profiles
Part K-2*:* Service Discovery Application Profile
Version 1.1, 22 February 2001, http://www.bluetooth.com/

[5] Bluetooth SIG, Specification of the Bluetooth System, Profiles
Part K-6: Headset Profile
Version 1.1, 22 February 2001, http://www.bluetooth.com/

[6] Bluetooth SIG, Specification of the Bluetooth System, Profiles
Part K-7: Dial-Up Networking Profile
Version 1.1, 22 February 2001, http://www.bluetooth.com/

[7] Bluetooth SIG, Specification of the Bluetooth System, Profiles
Part K-9: LAN Access Profile
Version 1.1, 22 February 2001, http://www.bluetooth.com/

[8] Bluetooth SIG, Specification of the Bluetooth System, Profiles
Part K-10: Generic Object Exchange Profile
Version 1.1, 22 February 2001, http://www.bluetooth.com/

[9] Bluetooth SIG, Specification of the Bluetooth System, Profiles
Part K-13: Synchronization Profile
Version 1.1, 22 February 2001, http://www.bluetooth.com/

[10] Bluetooth SIG, Personal Area Networking Profile
Version 0.95a, 26 June 2001, work in progress

[11] Bluetooth SIG, Bluetooth Security Architecture White Paper
Version 1.0, July 15 1999, http://www.bluetooth.com/

[12] User-Based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)
U. Blumenthal and B. Wijnen, RFC 2573, 1999

[13] PPP Extensible Authentication Protocol (EAP)
L. Blunk and J. Vollbrecht, RFC 2284, 1998

[14] The TLS Protocol Version 1.0
T. Dierks and C. Allen, IETF RFC 2246

[15] The Internet Key Exchange (IKE)
D. Harkins and D. Carrelm, RFC 2409, 1998

[16] An Architecture for Describing SNMP Management Frameworks
D. Harrington, P. Presuhn, and B. Wijnen, RFC 2571, 1999

[17] IrDA Object Exchange Protocol (IrOBEX) Specification with Published Errata
Version 1.2, Infrared Data Association, April 1999

[18] IrMC (Ir Mobile Communications) Specification with Published Errata
Version 1.1, Infrared Data Association, February 1999

[19] Security Architecture for the Internet Protocol
S. Kent and A. Atkinson, RFC 2401, 1998

[20] SNMP Applications
D. Levi, P. Meyer, and B. Stewart, RFC 2573, 1999

[21] The PPP Encryption Protocol (ECP)
G. Meyer, RFC 1968, 1996

[22] Remote Authentication Dial-In User Service (RADIUS)
C. Rigney et. al., RFC 2138, 1997

[23] PPP Challenge Handshake Authentication Protocol (CHAP)
W. Simpson, RFC 1994, 1996

[24] Using SRP for TLS Authentication
D. Taylor, Internet Draft draft-ietf-tls-srp-01.txt, June 29, 2001

[25] Microsoft PPP CHAP Extensions
G. Zorn and S. Cobb, RFC 2433, 1998