3GPP TSG SA WG3 Security — SA3#36 **S3-041150**

November 23-26, 2004, Shenzen, China

CR-Form-v7

CHANGE REQUEST

⌘ **TR 33.817 CR 001** ⌘**rev** **2** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network □

Title:	⌘	Bluetooth security and configuration considerations for Annex of TR 33.817
Source:	⌘	SA WG3
Work item code:	⌘	WLAN
Date:	⌘	15/11/2004
Category:	⌘	**B**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can
be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change: ⌘ The CR adds the background material on Bluetooth Security.

Summary of change: ⌘ Addition of background material in informative Annex by providing an overview of Bluetooth security and configuration considerations when used in the following context:

1. As an alterative access technology to 802.11 interworking with 3GPP networks in the same way as HIPERLAN/2 Security architecture is described in Annex A2 of TS33.234.
2. As a technology to implement the WLAN-UE Functional Split as described in section 4.2.4 of TS33.234.

Providing some details of Bluetooth

- Security Modes and Levels
- Authentication Key Hierarchy
- Processes for setting up keys
- Authentication and ciphering.

Configuration considerations in the context of WLAN interworking with references to published Bluetooth security analysis.

Consequences if not approved: ⌘ Background information on Bluetooth is missing.

Clauses affected: ⌘

		Y	N			
Other specs	⌘		X	Other core specifications	⌘	

affected:		**X**	Test specifications
		X	O&M Specifications
Other comments:	⌘		The table in the annex is informative showing a contrast of configuration considerations and recommendations. Some of the recommendations are guidance to the designers and some have been adopted as the requirements The remarks column specifies it.

~~********** FIRST CHANGE **********~~

~~2 References~~

~~[15] Bluetooth™ Security White Paper Bluetooth SIG Security Expert Group~~

~~http://grouper.ieee.org/groups/1451/5/Comparison%20of%20PHY/Bluetooth_24Security_Paper.pdf~~

~~[16] Markus Jakobsson and Susanne Wetzel "Security Weaknesses in Bluetooth" available at web site http://www.rsasecurity.com/rsalabs/staff/bios/mjakobsson/bluetooth/bluetooth.pdf.~~

~~[17] Thomas G. Xydis Ph.D. Simon Blake-Wilson "Security Comparison: BluetoothTM Communications vs. 802.11", available at web site http://www.ccss.isi.edu/papers/xydis_bluetooth.pdf~~

~~[18] Juha T. Vainio, "Bluetooth Security", Department of Computer Science and Engineering, Helsinki University of Technology, available at web site http://www.niksula.cs.hut.fi/~jiitv/bluesec.html~~

~~[19] Henrich C. Poehls, "Security Requirements for Wireless Networks and their Satisfaction in IEEE 802.11b and Bluetooth", Master's Thesis, Royal Holloway, University of London available at web site http://www.2000grad.de/impressum/Security_Requirements_for_Wireless_Networks_and_their_Satisfaction_in_IEEE_802_11b_and_Bluetooth.pdf~~

~~[20] LS on "Attack and countermeasures in a User Equipment functionality split scenario using Bluetooth"~~

~~http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_32_Edinburgh/Docs/ZIP/S3-040164.zip~~

~~[21] Red fang the Bluetooth hunter~~

~~http://www.atstake.com/research/tools/info_gathering/~~

~~[22] News - Red Fang "Bluetooth hack" not much use" - TDK available at web site http://www.newswireless.net/articles/0300910-bluestake.html~~

~~[23] "Specification of the Bluetooth System", Bluetooth, http://www.bluetooth.com/~~

~~[24] 3GPP TS 31.102: "Characteristics of the USIM application".~~

********** ~~NEXT~~FIRST CHANGE **********

Annex B (informative):

Additional Information on Bluetooth

B.1 Communication over local interface via a Bluetooth link

For SIM access via a Bluetooth link, the SIM Access Profile developed in Bluetooth SIG forum may be used. However it shall meet the following:

Requirements when Bluetooth is used for the Local Link.

With the SIM Access Profile, Bluetooth SIG specified functions which meets some of the requirements for Security Reuse. However, some requirements shall be added to the current SIM Access Profile specification to provide missing functionality and security level for Reuse:

1. The server shall allow itself and one additional device to access the card concurrently when the secure link is established and the enternal device has been authenticated.

2. Access to SIM, USIM, and ISIM shall be possible.

3. The local interface may need to provide integrity protection (Requirement No. 9, Requirement No. 13).

Editor's Note: As a result of an analysis it was decided during SA3 #31 that integrity protection over the Bluetooth link is probably not needed in the context of WLAN interworking because the encryption provides sufficient protection against man-in-the-middle attacks.

B.2 Device Management Requirements

New Mobile Devices as well as PDAs and Laptops are appearing with the ability to "talk" to each other creating Personal Area Networks (PANs), independent of the Mobile Operator's network. Supporting current standards such as Bluetooth, Infrared, 802.1Xx (and other emerging and future standards) necessitates the following requirements which assume security standards within the respective protocols such as utilizing. Challenge-Response Authentication, Stream Cipher Encryption and "trust" level controls.

1. Default Settings

a) The default settings of any device coming from the manufacturer shall always be set to "Do Not Auto Connect" or "Do Not Make Discoverable".

b) The user shall be aware that they are allowing their device to "be seen" by other devices.

2. Connection Confirmation

a) A device shall only accept a connection from another device after receiving a confirmation from the user indicating willingness to accept such a connection (i.e. there shall be no "auto-accept" feature on the device).

b) The requesting device shall represent itself via its Unique Identifier.

3. Unique Identifier

a) The user shall be required to provide a unique name (name other than "default") for the device in the setup menu of the connection protocol.

b) The ability to connect to another device shall only be enabled after the user provides a Unique Identifier. This Unique Identifier could be a PIN or Password. A device identity in a PAN enviornment (like Bluetooth) should not be generic, but unique. (This gives the user the ability to know if he is connecting to the right device among several devices in a given PAN environment).

4. Password Change

The user shall be required to change the passwordfrom the shipped default (e.g., [0000]) prior to first use. The password may apply to both a Bluetooth device as well as a mobile terminal.**5. Access Level Controls**

a) The user shall be able to configure and grant security access levels to their device. These access level controls may be "high security", "medium security", and "low security".

1. A high security level of access to a list of devices defined by the user (My Friends devices - Joes-T68, Abes-6820 etc.) for full data exchanges.

2. A mid level security that allows access to defined areas (receipt of low risk items - Pictures, SMS etc.).

3. A low security level of access for undefined devices that allow receipt of messages only (enable the receipt of text).

b) A selective level of access to a list of devices defined by Unique Identities and password; for data exchanges shall be provided.

c) An intermediate level of access that allows access to defined areas shall be provided (e.g., (U)SIM sharing feature but not AT command set, or, (U)SIM sharing feature and phone book etc).

d) An open level of access for undefined devices that allows receipt of messages only shall be provided.

Editor's note: A new Bluetooth profile is needed to fulfil these requirements. The version of the SIM Access Profile specification in the reference does not suffice to realize a functionally split WLAN-UE.

B.3 Communication over local interface via a Bluetooth link

1. The full 16 octet PIN shall be used for pairing and initialisation key establishment

2. Combination keys shall be used for link key generation.

3. The connection shall be terminated and restarted at least once a day to force the use of a new random number in the Bluetooth ciphering process to prevent key stream repeats

4. The use of a Separate Bluetooth interface/software stack for the local link that cannot be placed in discoverable mode by the user once the pairing process is complete may be considered for high security applications.

5. Only Bluetooth Version 1.2 shall be used which provides protection against interference from the WLAN interface in the same band shall be used

6. Deliberate denial of service attacks on the Bluetooth shall be minimised by reserving at least ***20*** channels for local link communication.

B.4 Introduction & Background

The Bluetooth technology provides peer-to-peer communications over short distances. In order to provide usage protection and information confidentiality, the system has to provide security measures both at the application layer and the link layer. This means that in each Bluetooth unit, the authentication and encryption routines are implemented in the same way. The following provides an informational guide on how these security measures are implemented.

B.5 Security Modes and Levels

Bluetooth enabled devices can operate in one of three different security modes as per the Bluetooth specifications:

- **Security Mode 1** - This is the most insecure security mode in which the Bluetooth device does not initiate any security procedure. It is in a ‘discovery’ mode, allowing other Bluetooth devices to initiate connections with it when in range.

- **Security Mode 2** - This mode enforces security after establishment of the link between the devices at the L2CAP level. This mode allows the setting up of flexible security policies involving application layer controls running in parallel with the lower protocols.

- **Security Mode 3** - This mode enforces security controls such as authentication and encryption at the Baseband level itself, before the connection is set up. The security manager usually enforces this onto the LMP.

Bluetooth allows security levels to be defined for both devices and services:

For **devices** there are two possible security levels. A remote device could either be a:

- **Trusted device** - Such a device would have access to all services for which the trust relationship has been set.

- **Untrusted device** - Such a device would have restricted access to services. Typically such devices would not share a permanent relationship with the other device.

For **services**, three levels of security have been defined.

- **Service Level 1** - services that require authorisation and authentication. Automatic access is only granted to trusted devices. Other devices need a manual authorisation.
- **Service Level 2** - services that require authentication only. Authorisation is not necessary.
- **Service Level 3** - services open to all devices; authentication is not required, no access approval required before service access is granted.

Note: The Bluetooth Architecture allows for defining security policies that can set trust relationships in such a way that even trusted devices can only get access to specific services and not to others.

B.6 Access Control

Fundamentally, the core Bluetooth protocols can be used to implement the following security controls to restrict access to services:

- Access to Services would need Authorisation (Authorisation always includes authentication). Only trusted devices would get automatic access.
- Access to Services would need only authentication. i.e. the remote device would need to get authenticated before being able to connect to the application.
- Access to Services would need encryption. The link between the two devices must be encrypted before the application can be accessed.

Bluetooth core protocols can only authenticate devices and not users. This is not to say that user based access control is not possible. The Bluetooth Security Architecture (through the Security Manager) allows applications to enforce their own security policies. The link layer, at which Bluetooth specific security controls operate, is transparent to the security controls imposed by the application layers. Thus it is possible to enforce user-based authentication and fine grained access control within the Bluetooth Security Framework.

B.7 Bluetooth Keys

Bluetooth security relies on symmetric keys for authentication and encryption. The keys involved include:

- Bluetooth Device Address – B8 bit address, unique to each Bluetooth device (BD_ADDR)
- Random number – 128 bit random number (may be pseudo-random), changes frequently (RAND)
- Initialisation Key (INIT)
- Unit Key (UNIT)
- Link Key (LINK)
- Encryption Key (ENC)
- Authentication Key (AUTH)

B.8 Processes for setting up keys

Further information on the protocols is described in Ref [19] with the full details available fromRef [24].

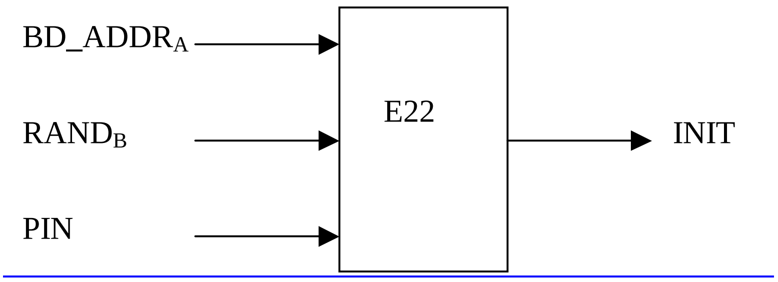
B.8.1 Initialisation Key Establishment

This protocol is used to exchange a temporary initialisation key, which is used to encrypt information during the generation of the encryption key.

For devices A and B:

1. A PIN is manually entered to each device.

2. Device A, having detected device B (and sees B’s Bluetooth device address) sends a random number to device B.
3. Both Bluetooth devices calculate an initialisation key, based on the random number sent by A, the Bluetooth device address of B and the shared PIN (uses algorithm E22).
4. Verification: A chooses a new random number and calculates a number based on the initialisation key, the new random number and B’s Bluetooth device address. This is sent to B.
5. B reverses the process using its Bluetooth device address, the initialisation key and the number sent and returns this.
6. A can now confirm the keys were shared successfully.
7. Repeat the last 3 steps with roles reversed, so B can confirm the same



Link key generation – Option 1 (Unit Key)

This is to share a link key, having established an initialisation key as above. In this case, one device is limited in memory (device A), so a ‘short cut’ is employed:

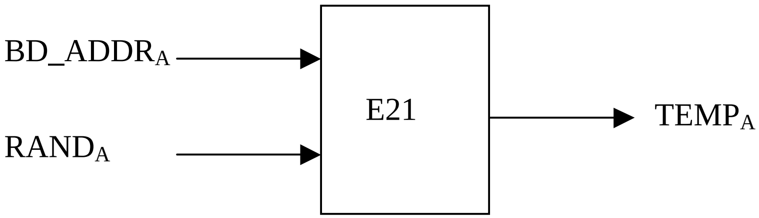
1. A encrypts its unit key with the initialisation key and sends this to B.
2. B decrypts the message with the initialisation key.
3. Both devices now have A’s unit key, and they use this as the link key. The initialisation key is now discarded.

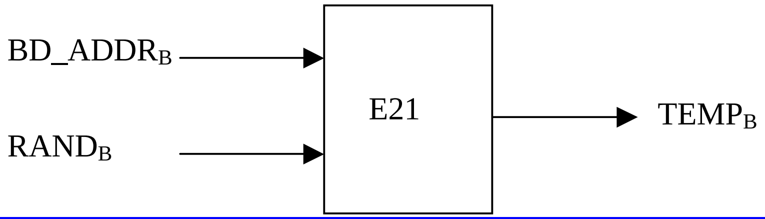
The problem with this is that if A now communicates with another device, say C, then this pair will use the same encryption key and B can read all their communications and impersonate A.

Link key generation – Option 2 (Combination Key)

This is an alternative to Option 1, and is recommended, assuming both devices are sufficiently capable. The result is a combination key.

1. Both devices generate a random number.
2. Device A computes a number based on its random number and Bluetooth device address, using algorithm E21.
3. Device B does the same with its own keys.
4. Both units encrypt their calculated numbers with their shared initialisation key and send them to each other.
5. Both devices now have both calculated numbers and combine them to create the link key – in this case, a combination key.
6. The link key is mutually verified. The initialisation key is no longer needed.



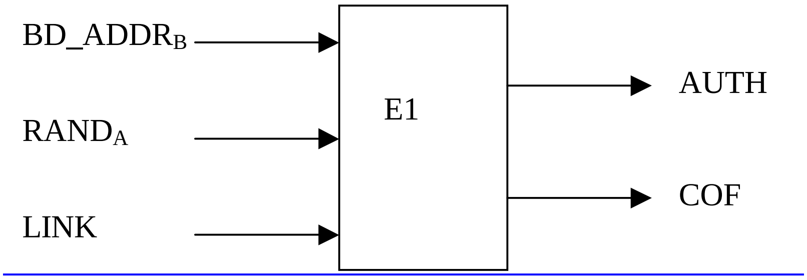


$$Temp_A \oplus Temp_B \rightarrow LINK$$

B.9 Authentication

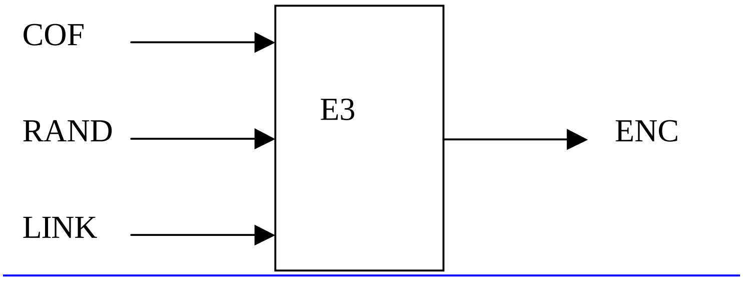
Once the link key has been set up, authentication can start. Here, device A is authenticating device B.

1. A sends a random 128 bit challenge to B.
2. B calculates a number using the challenge, its Bluetooth device address and the link key, under algorithm E1.
3. B returns just the 32 most significant bits to A.
4. A can now check these bits to authenticate B.
5. The remaining 96 bits are the Ciphering Offset Number (COF), used in encryption.
6. The roles of A and B can now be reversed.



B.10 Encryption (Confidentiality)

Every time this pair of Bluetooth devices starts an encrypted session, they calculate an encryption key. They use a random number, the link key and the Ciphering Offset Number (generated during authentication).



All data is encrypted, using algorithm E0 and the encryption key to encrypt the packets sent between devices providing confidentiality between the communicating devices.

B.11 Configuration Considerations

Ref.	Consideration	Recommendation	Remarks
1	Any key in Bluetooth depends either directly on its generation or for protective reasons on the Initialisation Key, which is built from a secret PIN. So if an attacker is able to capture the communications from the initialisation sequence onwards the attacker only has to find the right PIN to break the security of all keys, including the link encryption keys. A link key is used temporarily during initialization, known as the initialization key. This key is derived from the BD_ADDR, a PIN code, the length of the PIN (in octets), and a random number IN_RAND which a transmitted in clear over the air. This derived key becomes the CURRENT LINK KEY. The encryption engines in both devices must then be synchronized • An LMP_in_rand message is sent carrying the random number; both sides then use that to initialise their encryption engines • Next the verifier sends and LMP_au_rand message containing the random number to be authenticated by the claimant. • The claimant encrypts this number using its CURRENT LINK KEY and then returns the encrypted number in a secure response message LMP_sres. • The verifier encrypts the random number from LMP-au_rand with its CURRENT LINK KEY and compares it with the encrypted version in LMP_sres. • Thus the verifier can decide whether both sides share the same link key without the link key ever being transmitted on air. Once Master and Slave know that they share a secret key, they could use that key for encrypting traffic. But if data with a pattern is sent then it is possible to eventually crack the link key. Hence the use of dynamic derived keys either unit and combination keys. The combination key is the combination of two numbers generated in device A and B, respectively. Each device generates a random number which are protected during the on air exchange by XORing with the CURRENT LINK KEY The same procedure is invoked regularly during normal operation to refresh the link keys and prior to encryption start to modify the encryption keys to address the key stream repeat issue. Hence other than the PIN, all other information that contributes to the authentication /ciphering is publicly known or protected with a strength equal to that of the PIN	The full 16 octet PIN shall be used which shall be unique to each device. Out of band secure distribution methods shall be considered. Ref: [~~16~~C2] [~~17~~C3] [~~18~~C4] [~~19~~C5] [~~20~~C6]	

Ref.	Consideration	Recommendation	Remarks
2	Unit keys are static and only changed when the Bluetooth device is reset. If an attacker is able to authenticate, or at least perform the first 3 steps of the initialisation procedure, he is able to learn the Unit Key. As this is the Link Key that the attacked device also uses for all other connections the attacker can masquerade as the attacked device, or eavesdrop later encrypted transmissions	Combination keys shall be used Ref [~~18~~C4] [~~20~~C6]	This recommendation has been requested to be adopted as a requirement in the CR on section B.3. See section B.3 requirement 2
3	Key stream reuse The clock value is also used to calculate a new seed, and therefore a new key stream, for each packet. A key stream reuse will occur after approximately one day. The clock value is a 28-bit counter that is incremented every 312.5 s, so 228 * 312.5 s = 23.30 h. The key stream also depends on a random value, which is exchanged when encryption is enabled. So to prevent encryption under the same key stream more than once, Bluetooth devices do not need to generate a new encryption key, it would be sufficient if they would restart the encryption once a day, to use a new random number. The Bluetooth master always has assurance of encryption key freshness as it contributes a nonce to the computation of the encryption key at the start of encryption. Bluetooth provides mutual entity authentication and mutual key authentication. Mutual authentication is performed as a succession of two unilateral authentications. A value ACO is computed as a result of an authentication. The initiator of a unilateral authentication inputs a nonce to the computation of ACO, the responder does not. The ACO value from the authentication performed last is used to derive the encryption key. So, the initiator of the last authentication also has assurance of encryption key freshness, as long as it can be assured to have initiated the last authentication. The connection shall be terminated and restarted at least once a day to force the use of a new random number from a command from the network The encryption key generation could be changed so as to give assurance of encryption key freshness also to the slave.	Ref: [~~20~~C6] [~~21~~C7]	This recommendation has been requested to be adopted as a requirement in the CR on section B.3See section B.3 requirement 3 Guidance to the designer (may be included in the user guide and/or a message may be generated and displayed by the device informing the user to terminate and restart the connection)

Ref.	Consideration	Recommendation	Remarks
4	Replay of old messages due to Lack of Integrity protection in the Bluetooth security design. Just taking over an authenticated connection will not be so easy if the connection is encrypted, as the encryption key is based on the link key. Therefore a Bluetooth device knows that valid encrypted packets can only be generated by a device in possession of the valid link key (either itself or the authenticated device). If different link keys are established for each combination of two Bluetooth devices this means the attacker cannot generate new messages. But as the integrity of packets is not protected an attacker might replay old messages. Bluetooth Clock: the Bluetooth clock value is input to the encryption algorithm, so the attacker needs to reset the Bluetooth clock before replaying a message to the target. The Bluetooth master controls the Bluetooth clock and can reset it.	Ensure that encryption is applied and managed according to recommendations outlined in this document. Support enhancement of the Bluetooth security specification with Integrity by message authentication code. Ref: [~~20~~C6] [~~21~~C7]	Guidance to the designer
5	Loss of location privacy in discoverable mode The Bluetooth device's unique base address is freely broadcasted for example during the inquiry procedure. As this is a permanent unique identifier of a personal device, tracking is easy if the device is in discoverable mode. By observing the time, rate, length, maybe even source or destination of messages an attacker can deduce confidential information. Privacy issues arise if the attacker can observe a fixed source identifier, which could be traced and associated with a user. An attacker sends messages to the wireless network or actively initiates communication sessions. Then by observing the time, rate, length, sources or destinations of messages on the wireless transmission medium an attacker can deduce confidential information. An attacker does not require reading the actual data, but for some users the sheer information that they are communicating is considered to be confidential.	A warning should be implemented to inform users about vulnerabilities that are inherent with Bluetooth devices in discoverable mode. c.f. Bluesnarfing and Bluejacking Separate Bluetooth interface/software stack that cannot be placed in discoverable mode by the user once the pairing process is complete. What the end user does with the other interface is then up to the end user. Ref: [~~17~~C3] However, non-discoverable mode can also be attacked see concern 6 below.	This recommendation has been requested to be adopted as a requirement in the CR on section B.3 See section B.3 requirement 4

Ref.	Consideration	Recommendation	Remarks
6	Finding non-discoverable Bluetooth devices by brute forcing the last six bytes of the devices Bluetooth address and sending a read_remote_name (Redfang Tool)	Implement a warning to users about vulnerabilities that are inherent with Bluetooth devices in non discoverable mode Review 3GPP requirement for Anonymity Mode Ref: [~~22~~C8] [~~23~~C9]	
7	Use of Narrow band Jammer to force Bluetooth V1.2 devices to “sterilise” all channels on the assumption that they need to be avoided due to interference from 802.11 I devices	Need to ensure that that all frequencies are not used up.	This recommendation has been requested to be adopted as a requirement in the CR on section B.3 See section B.3 requirement 6
8	Bluetooth V1.1 has a problem with the Inquiry protocol in that there was a 1 in 10 chance that the devices would not connect.	In the context of 3GPP WLAN Interworking only Bluetooth Version 1.2 shall be used.	This recommendation has been requested to be adopted as a requirement in the CR on section B.3See section B.3 requirement 5

B.12 Bibliography

[C1] Bluetooth™ Security White Paper Bluetooth SIG Security Expert Group

http://grouper.ieee.org/groups/1451/5/Comparison%20of%20PHY/Bluetooth_24Security_Paper.pdf

[C2] Markus Jakobsson and Susanne Wetzel “Security Weaknesses in Bluetooth” available at web site http://www.rsasecurity.com/rsalabs/staff/bios/mjakobsson/bluetooth/bluetooth.pdf.

[C3] Thomas G. Xydis Ph.D. Simon Blake-Wilson “Security Comparison: BluetoothTM Communications vs. 802.11”, available at web site http://www.ccss.isi.edu/papers/xydis_bluetooth.pdf

[C4] Juha T. Vainio, “Bluetooth Security”, Department of Computer Science and Engineering, Helsinki University of Technology, available at web site http://www.niksula.cs.hut.fi/~jiitv/bluesec.html

[C5] Henrich C. Poehls, “Security Requirements for Wireless Networks and their Satisfaction in IEEE 802.11b and Bluetooth”, Master’s Thesis, Royal Holloway, University of London available at web site http://www.2000grad.de/impressum/Security_Requirements_for_Wireless_Networks_and_their_Satisfaction_in_IEEE_802_11b_and_Bluetooth.pdf

[C6] LS on “Attack and countermeasures in a User Equipment functionality split scenario using Bluetooth”

http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_32_Edinburgh/Docs/ZIP/S3-040164.zip

[C7] Red fang the Bluetooth hunter

http://www.atstake.com/research/tools/info_gathering/

[C8] News - Red Fang "Bluetooth hack" not much use" - TDK available at web site http://www.newswireless.net/articles/0300910-bluestake.html

[C9] "Specification of the Bluetooth System", Bluetooth, http://www.bluetooth.com/

[C10] 3GPP TS 31.102: "Characteristics of the USIM application".