3GPP TSG SA WG3 Security — S3#34 **S3-040468**
July 6 - 9, 2004, Acapulco, Mexico

3GPP TSG-SA3#33 **Tdoc ⌘S3-030379**

10th – 14th May, 2004 Beijing, China

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.234 CR CRNum** ⌘**rev -** ⌘ 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⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Impact of TR 33.817 (Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces). Bluetooth security and configuration considerations for Annex A4 of TS 33.234 (Wireless Local Area Network (WLAN) interworking security)
Source:	⌘	Toshiba, BT and supporting Companies
Work item code:	⌘	(U)SIM Reuse
Date:	⌘	28/05/2004
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:	⌘	TS 33.234 currently does not consider the Reuse of a Single SIM, USIM, or ISIM by peripheral devices on local interfaces to access multiple networks. This aspect has been studied in the feasibility study report (i.e. TR~~S~~ 33.817). Annex A4 of TS 33.234 is empty in its present version. The CR adds the background material and fulfils the intent of the annex.
Summary of change:	⌘	Some minor changes mostly the insertion of reference of TR 33.817 to accommodate the additional feature. Addition of background material in informative Annex A4 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:	⌘	New feature could not be supported. And the specification will be incomplete that may result in inappropriate Bluetooth configurations in the WLAN-UE functional split case. This may result in a compromise of WLAN interworking security

Clauses affected:	⌘	2, 4.1.4, 4.2.4.1, 4.2.4.3, 6.1.1, 6.1.5, C3.1 and Annex A4			
Other specs affected:	⌘	**Y** / **N**	Other core specifications Test specifications O&M Specifications	⌘	
Other comments:	⌘	The table ~~As~~ 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 beed~~n~~ adopted as the requirements The remarks column specifies it. ~~are in the form of recommendations and guidance to designers. CR's may follow to transfer specific requirements to the main body of the specification~~.			

***** Start of change *****

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TR 22.934: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking".

[2] 3GPP TR 23.934: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) Interworking; Functional and architectural definition".

[3] draft-ietf-eap-rfc2284bis-06.txt, October 2003: "PPP Extensible Authentication Protocol (EAP)".

[4] draft-arkko-pppext-eap-aka-11, October 2003: "EAP AKA Authentication".

[5] draft-haverinen-pppext-eap-sim-12, October 2003: "EAP SIM Authentication".

[6] IEEE Std 802.11i/D7.0, October 2003: "Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security".

[7] RFC 2716, October 1999: "PPP EAP TLS Authentication Protocol".

[8] SHAMAN/SHA/DOC/TNO/WP1/D02/v050, 22-June-01: "Intermediate Report: Results of Review, Requirements and Reference Architecture".

[9] ETSI TS 101 761-1 v1.3.1B: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 1: Basic Data Transport".

[10] ETSI TS 101 761-2 v1.2.1C: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 2: Radio Link Control (RLC) sublayer".

[11] ETSI TS 101 761-4 v1.3.1B: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 4 Extension for Home Environment".

[12] ETSI TR 101 683 v1.1.1: "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview".

[13] 3GPP TS 23.234: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) Interworking; System Description".

[14] RFC 2486, January 1999: "The Network Access Identifier".

[15] RFC 2865, June 2000: "Remote Authentication Dial In User Service (RADIUS)".

[16] RFC 1421, February 1993: "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures".

[17] Federal Information Processing Standard (FIPS) draft standard: "Advanced Encryption Standard (AES)", November 2001.

[18] 3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing and identification".

[19] IEEE P802.1X/D11 June 2001: "Standards for Local Area and Metropolitan Area Networks: Standard for Port Based Network Access Control".

[20] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[21] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[22] CAR 020 SPEC/0.95cB: "SIM Access Profile, Interoperability Specification", version 0.95VD.

[23] draft-ietf-aaa-eap-03.txt, October 2003: "Diameter Extensible Authentication Protocol (EAP) Application".

[24] RFC 3588, September 2003: "Diameter base protocol".

[25] RFC 3576, July 2003: "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)".

[26] RFC 3579, September 2003: "RADIUS (Remote Authentication Dial In User Service) Support for Extensible Authentication Protocol (EAP)".

[27] draft-ietf-eap-keying-01.txt, November 2003: "EAP Key Management Framework".

[28] E. Barkan, E. Biham, N. Keller: "Instant Ciphertext-Only Cryptoanalysis of GSM Encrypted Communication", Crypto 2003, August 2003.

[29] draft-ietf-ipsec-ikev2-12.txt, January 2004, "Internet Key Exchange (IKEv2) Protocol".

[30] RFC 2406, November 1998, "IP Encapsulating Security Payload (ESP)".

[31] draft-ietf-ipsec-ui-suites-04.txt, August 2003, "Cryptographic Suites for IPsec".

[32] 3GPP TR 33.817 "~~"~~Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces ~~(Release 6)~~"~~"~~

~~[33] 3GPP TS 31.102: "Characteristics of the USIM application".~~

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

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

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

[35] 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

[36] 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

[37] 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

[38] 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

[39] Red fang the Bluetooth hunter

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

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

[41] “Specification of the Bluetooth System”, Bluetooth, http://www.bluetooth.com/

[42] 3GPP TS 31.102: "Characteristics of the USIM application".

***** End of change *****

***** Start of change *****

4.1.4 Network elements

The list below describes the access control related functionality in the network elements of the 3GPP-WLAN interworking Reference Model:

- The **WLAN-UE**, equipped with a UICC (or SIM card), for accessing the WLAN interworking service):
  - May be capable of WLAN access only;
  - May be capable of both WLAN and 3GPP System access;
  - May be capable of simultaneous access to both WLAN and 3GPP systems;

  Editors note: definition of simultaneous access still TBA with SA1- LS in S3 030169] Reply to SA2 in S3-030188 provides some clarification. (Already studied and declared feasible in TR 33.817[32], however the mechanisms still need to be defined).

  - May be a laptop computer or PDA with a WLAN card, UICC (or SIM card) card reader, and suitable software applications;
  - May be functionally split over several physical devices, that communicate over local interfaces e.g. Bluetooth, ~~IR~~Infrared or serial cable interface; (this alternative is feasible as per TR-33.817[32])

  Editors note: All these alternatives must be carefully studied from a security perspective.

- The **AAA proxy** represents a logical proxying functionality that may reside in any network between the WLAN and the 3GPP AAA Server. These AAA proxies are able to relay the AAA information between WLAN and the 3GPP AAA Server.
  The number of intermediate AAA proxies is not restricted by 3GPP specifications. The AAA proxy functionality can reside in a separate physical network node; it may reside in the 3GPP AAA server or any other physical network node;

- The **3GPP AAA server** is located within the 3GPP network. The 3GPP AAA server:
  - Retrieves authentication information from the HLR/HSS of the 3GPP subscriber's home 3GPP network;
  - Authenticates the 3GPP subscriber based on the authentication information retrieved from HLR/HSS. The authentication signalling may pass through AAA proxies;
  - Communicates authorisation information to the WLAN potentially via AAA proxies.
- The **Packet Data Gateway (PDGW)** enforces tunnel authorization and establishment with the information received from the 3GPP AAA via the Wm interface.

NOTE: The **WLAN Access Gateway (WAG)** responsibilities for security issues are related to tunnel establishment but this decision is pending to be taken.

***** End of change *****

***** Start of change *****

4.2.4 WLAN-UE Functional Split

4.2.4.1 General

In the case when the WLAN-UE, (integrated ~~equipped~~ with a UICC ~~(~~or SIM card~~;)~~, or linked by Bluetooth or USB (Universal Serial Bus) for accessing the WLAN interworking service), is functionally split over several physical devices one device holding the card, and one device providing the WLAN access, that communicate over local interfaces e.g. Bluetooth, ~~IR~~Infrared or serial cable interface, then it ~~is~~ shall be:

- Possible to re-use existing UICC and GSM SIM cards; (as demonstrated in TR 33.817[32], however, improvements are needed at least in UICC card), and
- The UE functional split shall be such that attacking the CS or PS domain of GSM or UMTS by compromising the device providing the WLAN access is at least as difficult as attacking the CS or PS domain by compromising the card holding device.

Editors note: The requirement is fulfilled if at least the master keys for EAP-AKA and EAP-SIM, as specified in [4] and [5], are computed either on the card or in the card holding device.

Editor's note: The termination point of EAP is for further study e.g. if EAP-AKA and EAP-SIM shall terminate in the TE e.g. laptop computer. The decision on the termination point shall take into account the requirements in this subsection.}. LS sent to Bluetooth Architecture Review Board (BARB), Bluetooth CAR group and Bluetooth Security Expert Group in S3-030780

***** End of change *****

***** Start of change *****

4.2.4.2 Generic ~~S~~security requirements on local interface

The security functionality required on the terminal side for WLAN-3G interworking may be split over several physical devices that communicate over local interfaces TR 33.817~~.~~ [32]. According to "TR 33.817 [32], the (U)SIM card may reside in a 3GPP UE (acting as a (U)SIM "server") and be accessed by a WLAN-UE through Bluetooth, Infrared or a USB (Universal Serial Bus) cable or some other similar wired or wireless interconnect technology (acting as the (U)SIM "client"). This would facilitate the user to get simultaneous WLAN and 3GPP access with the same (U)SIM. If this is the case, then the following requirements shall be satisfied:

1. —Any local interface shall be protected against eavesdropping, attacks on security-relevant information. This protection may be provided by physical or cryptographic means. For cryptographic means, the encryption key length shall be at least 128 bits.

2. —The endpoints of a local interface should be authenticated and authorised. The authorisation may be implicit in the security set-up. Keys used for local interface transport security shall not be shared across local interface links. Each local interface shall use unique keys. (For example in Bluetooth, Combination of Link keys shall be used. In case of Bluetooth, the keys may change when a new SIM Access Profile connection is established).

3. —The involved devices shall be protected against eavesdropping, undetected modification attacks on security-relevant information. This protection may be provided by physical or cryptographic means.

4. —The device without (U)SIM shall be capable of discovering the device(s) with (U)SIM in its proximity.

5. —The peripheral device without (U)SIM shall be capable of communicating with the U(SIM) only if the device containing (U)SIM is switched on and a (U)SIM is powered on. Furthermore the device without (U)SIM shall not be allowed to change the status of the device with (U)SIM, or the (U)SIM, e.g. to reset it, or to switch its power on or off.

6. —The peripheral device without the (U)SIM shall be capable of detecting the presence and availability of the (U)SIM on the device containing it. It shall also have the ability to terminate an authenticated network sessions when, the (U)SIM is no longer accessible within a short monitoring time period as defined in TS 31.102 [~~33~~42].

7. —User shall have the capability to shut off sharing of (U)SIM feature. The owner of the device, holding the (U)SIM shall authorize its use.

8. —Integrity and privacy of signalling between the WLAN system and the 3GPP core network shall be supported. Leakage of (U)SIM information to the user, or any third party over the wireless interface (Bluetooth/WLAN) is the major security threat. This leakage of information shall be guarded against.

9. —Whenever someone tries to remotely access a (U)SIM some sort of alert shall be sent, e.g. a message shall be displayed informing the user of the attempted access. The user can then decide whether the access is authorized and can allow or disallow it. The security level shall be the same or better than present GSM System or as defined by IETF (EAP-SIM, EAP-AKA) and shall apply to Circuit Switched (CS) domain as well as Packet Switched (PS) domain.

10. —It shall be possible to simultaneously access both WLAN and 3GPP radio access technologies. I.e., It shall support simultaneous calls on two different air interfaces. For example, the UE might use the WLAN for data services (internet access) together with the 3GPP system for a speech call. The UE and the WLAN and 3GPP systems might elect to use both access technologies simultaneously in order to balance traffic, system capabilities or for radio resource management.

11. —The UICC bearing device shall be responsible for serializing access to the (U)SIM Application/Data.

12. —The user shall be able to select (U)SIM and TEs as part of their user equipment combination.

13. —A standardized API for access to capabilities provided by an MT (TE) towards a TE (MT) across Operating Systems shall be provided.

14. —UICC presence detection shall be supported via the local interface. The local interface may need to address Issue No. 2, see [32] on Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces (Release 6)e.g. by retransmission of the STATUS command.

15. —Security Reuse shall be consistent with current security arrangements for Release 6 and ensure that user security is not compromised.

16. —Applications/Data information could be retrieved from (U)SIM, provided that (U)SIM is inserted in a 3GPP ME. When the (U)SIM is re-used over local interfaces, further access control on the Applications/Data information shall be applied by the 3GPP ME bearing the (U)SIM.

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

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

19. 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).

20. The requesting device shall represent itself via its Unique Identifier.

21. 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.

22. The ability to connect to another device shall only be enabled after the user provides a Unique Identifier.

23. If default passwords are used, then the user shall be required to change the password from the shipped default (e.g., [0000]) prior to first use.

24. The user shall be able to configure and grant security access levels to their device.

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

26. An intermediate level of access that allows access to defined areas shall be provided.

27. An open level of access for undefined devices that allow receipt of messages only shall be provided.

Editor note: The version of the SIM Access Profile specification in the reference needs to be updated, if SA3 decides that a new version is required.

Editors note: It was agreed at SA3#31 that for WLAN interworking, modification of EAP parameters on the Bluetooth interface will cause EAP to fail in the network or on the USIM. It was therefore agreed to remove the "undetected modification" requirement from this TS.

***** End of change *****

***** Start of change *****

4.2.4.3 Communication over local interface via a Bluetooth link

For SIM access via a Bluetooth link, the SIM Access Profile developed in ~~BLUETOOTH~~Bluetooth SIG forum may be used. See [22] and 3GPP TR 33.817 [~~23~~32]. However it shall meet the following:

~~Potential~~ Requirements for ~~for~~ when ~~-~~Bluetooth is used for the local link

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

1. ~~1.~~ The server shall allow itself and at least one additional device to access the card concurrently (Requirement No 12 in [32])~~).~~

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

3. ~~3.~~ The local interface may need to provide integrity protection (Requirement No. 9, Requirement No. 16~~)~~ in [32]).

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.

4. ~~4.~~ Mandatory security requirements for the pairing shall be specified to be enforced by the ME. This will ensure local interface security (Requirement No. 1, Requirement No. 16 in [32])~~). Users may not be aware of the fact that a short PIN does not provide adequate protection against brute-force attacks.~~

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

6. The initialisation key establishment PIN shall be unique to each device.

7. Out of band secure distribution methods shall be used for the initialisation key establishment PIN

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

9. 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

10. Users shall be informed in the set up instructions about vulnerabilities that are inherent with Bluetooth devices in discoverable mode.

11. 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.

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

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

~~NOTE: This list may not be exhaustive.~~

~~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 FHSS (Frequency Hopping Spread Spectrum), Challenge-Response Authentication, Stream Cipher Encryption and "trust" level controls.~~

~~1. Default Settings~~

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

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

~~2. Connection Confirmation~~

~~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).~~

~~The requesting device shall represent itself via its Unique Identifier.~~

~~3. Unique Identifier~~

~~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.~~

~~The ability to connect to another device shall only be enabled after the user provides a Unique Identifier.~~

~~**4. Password Change**~~

~~The user shall be required to change the password from the shipped default (e.g., [0000]) prior to first use.~~

~~**5. Access Level Controls**~~

~~The user shall be able to configure and grant security access levels to their device.~~

~~A selective level of access to a list of devices defined by Unique Identities and password; for data exchanges.~~

~~An intermediate level of access that allows access to defined areas.~~

~~An open level of access for undefined devices that allows receipt of messages only.~~

~~Editor note: The version of the SIM Access Profile specification in the reference needs to be updated, if SA3 decides that a new version is required.~~

***** End of change *****

***** Start of change *****

6.1.1 USIM-based WLAN Access Authentication

USIM based authentication is a proven solution that satisfies the authentication requirements from section 4.2. This form of authentication shall be based on EAP-AKA (ref. [4]), as described in section 6.1.1.1.

Editor's note: also see section 4.2.4 on WLAN-UE Functional Split, and [32] on Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces (Release 6).

***** End of change *****

***** Start of change *****

6.1.5 Mechanisms for the set up of UE-initiated tunnels (Scenario 3)

- The WLAN UE and the PDG use IKEv2, as specified in [ikev2], in order to establish IPSec security associations.
- Public key signature based authentication with certificates, as specified in [ikev2], is used to authenticate the PDG.
- EAP-AKA within IKEv2, as specified in [ikev2, section 2.16], is used to authenticate WLAN UEs, which contain a USIM. Or WLAN UEs that do not contain (U)SIM but can talk over local link to the device containing (U)SIM as per scenarios described in TR 33.817[32].
- EAP-SIM within IKEv2, as specified in [ikev2, section 2.16], is used to authenticate WLAN UEs, which contain a SIM and no USIM. Or WLAN UEs that do not contain (U)SIM but can talk over local link to the device containing (U)SIM as per scenarios described in TR 33.817[32].

***** End of change *****

***** Start of change *****

C.3.1 Attacks at the Victim's WLAN UE

Open platform terminals may be infected by viruses, Trojan horses or other malicious software. The software operates without the knowledge of the user on his terminal, and can be used for different types of attacks:

- If the user has credentials stored on a smart card connected to his terminal, a Trojan residing in the terminal can make fake requests to the smart card and send challenge-response results to another MS. For example, the owner of the latter MS could then get access with the stolen credentials.

NOTE: This attack is performed inside the terminal, and it is independent of the external link between the terminal and the smart card reader, which can be secured or assumed to be physically secure.

- Trojans may perform all the usual activities: monitor the user's keyboard or sensitive data, and forward the information to another machine.

- Malicious software can be used to perform Distributed DoS (DDoS) attacks. That is, several instantiations of the software (residing on different hosts) synchronise and start a DoS attack simultaneously against a target.

- Malicious software could be trying to connect to different WLANs, just to annoy the user.

Alternatively, the (U)SIM in the cellular phone can be used remotely from the WLAN client through a serial, infrared, or Bluetooth connection,~~;~~ ~~33.817~~TR 33.817[32], in order to use the phone as a smart card reader. As the terminal must access the (U)SIM in the phone, the link in between must be secure. Both cable and ~~IR~~Infrared can be assumed physically secure, and Bluetooth will depend highly on the current Bluetooth security mechanism.

***** End of change *****

******NEXT CHANGED SECTION******

A.4 Bluetooth

***** BEGIN SET OF CHANGES *****

A 4.1 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.

A 4.2 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.

A 4.3 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.

A 4.4 Bluetooth Keys

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

- Bluetooth Device Address – a 48 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)

A 4.5 Processes for setting up keys

Further information on the protocols is described in Ref [37] with the full details available from

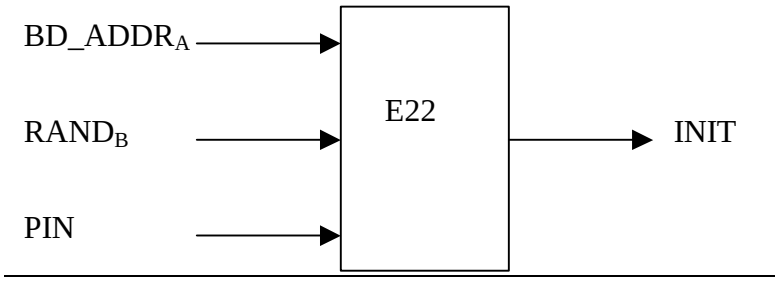
Ref [42].

A 4.5.1 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:

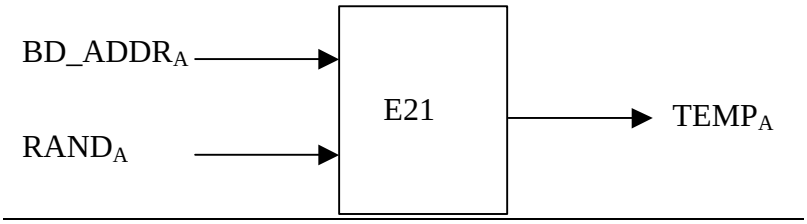
1. A encrypts its unit key with the initialisation key and sends this to B.
2. B decrypts the message with the initialisation key.
3. Both devices now have A's unit key, and they use this as the link key. The initialisation key is now discarded.

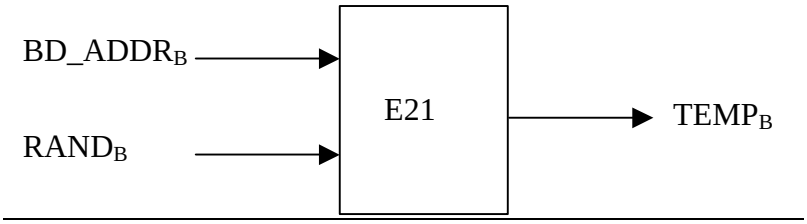
The problem with this is that if A now communicates with another device, say C, then this pair will use the same encryption key and B can read all their communications and impersonate A.

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.



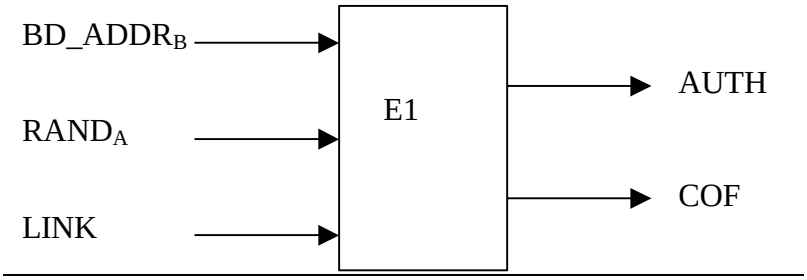


$$Temp_A \oplus Temp_B \rightarrow LINK$$

A 4.6 Authentication

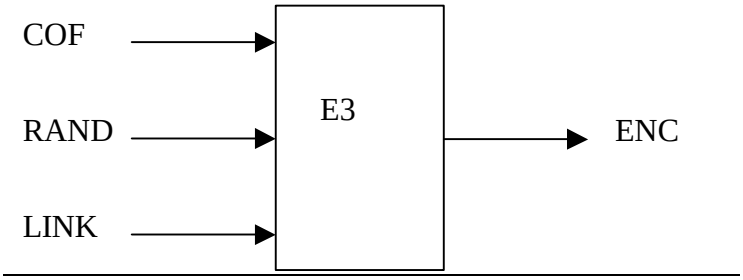
Once the link key has been set up, authentication can start. Here, device A is authenticating device B.

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.



A 4.7 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.

A4.8 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: [34] [35] [36] [37] [38]	This recommendation has been adopted as a requirement See section 4.2.4.3 requirement 5 and requirement 6 This recommendation has been adopted as a requirement See section 4.2.4.3 requirement 7

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 [36] [38]	This recommendation has been adopted as a requirement. See section 4.2.4.3 requirement 8
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: [38] [39]	This recommendation has been adopted as a requirement See section 4.2.4.3 requirement 9 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: [38] [39]	Guidance to the designer This recommendation has been adopted as a requirement See section 4.2.4.3 requirement 3
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: [35] However, non-discoverable mode can also be attacked see concern 6 below.	This recommendation has been adopted as a requirement See section 4.2.4.3 requirement 10 This recommendation has been adopted as a requirement See section 4.2.4.3 requirement 11

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: [40] [41]	This recommendation has been adopted as a requirement See section 4.2.4.3 requirement 10
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 adopted as a requirement See section 4.2.4.3 requirement 13
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 adopted as a requirement See section 4.2.4.3 requirement 12

**** END SET OF CHANGES *****