3GPP TR 33.817 V6.1.0 (2004-12)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces (Release 6)

Keywords
UMTS, WLAN, Service, Terminal, USIM

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

Wireless Local Area Networks (WLANs), first envisioned as a way to offer convenient access within enterprise networks, has now become popular installations in public spaces, and residences alike. This drift has dramatically altered the landscape of wireless data access. Not only their emergence, but also the potential interworking of public WLANs with 3G systems has become a topic of increasing importance and urgency for the entire wireless community.

The intent of 3GPP-WLAN Interworking is to extend 3GPP services and functionality to the WLAN access environment. Thus the WLAN effectively becomes a complementary radio access technology to the 3GPP system. Potential areas of interworking between a 3GPP system and WLAN include common authentication, authorization, and accounting functions. Under these state of affairs the User Equipment used to access different networks (3GPP, WLAN) may be implemented over a number of physical devices e.g. PC or PDA reusing (U)SIM Security on Local Interfaces.

The 3G-WLAN interworking requirements specified in [2] requires the ability for a SIM or USIM to be used for providing common access control and charging for WLAN and 3G services using the 3GPP system infrastructure. The current specifications of SIM and USIM in 3GPP assume a one-to-one association between the UICC and the Mobile Equipment (ME) to constitute the User Equipment (UE). Though this assumption holds in some UE architecture models, but do not hold in some models that are derived from the 3G-WLAN interworking requirements [2]. Here are some examples where such a one-to-one association is not possible when we consider WLAN to be a separate MT function.

- (U)SIM inside a GPRS/UMTS PC card module is used for WLAN authentication on a Laptop or PDA in addition to its use for GPRS/UMTS authentication.
- (U)SIM inside a GSM/UMTS terminal is used for WLAN authentication on a Laptop or PDA over a Bluetooth local link, in addition to its use for GSM/UMTS authentication.
- (U)SIM inside Dual-mode GPRS and WLAN terminal is used for WLAN authentication in addition to GSM authentication (Assuming WLAN and GPRS are separate MT functions).
- (U)SIM inside a Triple-Mode UMTS, GPRS, WLAN terminal used for WLAN authentication in addition to UMTS and GPRS authentication.
- (U)SIM inside a USB or PC Card UICC reader module is used to authenticate a WLAN session using a Laptop or PDA.

For these diverse usage models the specific security threats and issues need to be studied and appropriate security requirements need to be specified to counteract the threats. This document studies the specific security threats, issues and appropriate security requirements to counteract the threats and surmount the issues.

1 Scope

This Feasibility Study report conducts a threat analysis and determines the feasibility of Reuse of a Single SIM, USIM, or ISIM by peripheral devices on local interfaces to access multiple networks. Most important for this Reuse is the authentication and key agreement (AKA) function provided by these applications. The peripheral devices include 3GPP and WLAN devices that function as integrated or attachable peripherals on Laptops or PDAs or other mobile data devices. The multiple access networks of interest correspondingly include 3GPP and WLAN type networks. The objective of this study is to realize the diverse usage models with multiple external (wired or wireless) interfaces from a security point of view, without incorporating significant changes to the 3GPP and WLAN infrastructure. It also studies the impact on current security specifications for 3GPP, especially given that some issues have already been identified surrounding key setting procedures, USIM sequence number synchronization, UICC presence detection/UICC application presence detection and termination of the UICC usage etc. It also studies additional user authentication requirements (e.g. PINs) when used over local interfaces like Bluetooth, IR or USB. Further more it studies the impact on having many entities using the same security mechanism and any 3GPP core network elements. Reuse of security functions provided by applications on the UICC does not have an impact on ownership and control of the UICC, which remains with the issuer of the UICC. This Feasibility Study may be used as a basis for future CRs to TS 33.234 as and when any of the proposals are developed by SA WG3.

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

[2] 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".

[3] 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".

[4] 3GPP TS 33.234: "3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; 3G Security; Wireless Local Area Network (WLAN) Interworking Security".

[5] 3GPP TS 51.011 (Release 4): "3rd Generation Partnership Project; Technical Specification Group Terminals; Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface".

[6] 3GPP TS 42.017 (Release 4): "3rd Generation Partnership Project; Technical Specification Group Terminals; Subscriber Identity Modules (SIM); Functional characteristics".

[7] 3GPP TS 22.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description, Stage 1".

[8] 3GPP TS 22.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for the Internet Protocol (IP) multimedia core network subsystem; Stage 1".

[9] 3GPP TS 23.101 (Release 4): "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General UMTS Architecture".

[10] 3GPP TS 24.002: "3rd Generation Partnership Project; Technical Specification Group Core Network; GSM - UMTS Public Land Mobile Network (PLMN) Access Reference Configuration".

[11] 3GPP TR 22.944: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Report on Service Requirements for UE Functionality Split".

[12] Mobile Electronic Transactions - Personal Transaction Protocol [MeT PTP], Version 1.0.

[13] 3GPP TS 33.220: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[14] 3GPP TS 33.221: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Support for Subscriber Certificates".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following definitions apply:

Home WLAN: The WLAN that is interworking with the HPLMN of the 3GPP - WLAN interworking user.

Interworking WLAN: WLAN that interworks with a 3GPP system.

Visited WLAN: An interworking WLAN that interworks only with a visited PLMN.

WLAN coverage: An area where wireless local area network access services are provided for interworking by an entity in accordance with WLAN standards.

WLAN roaming: The ability for a 3GPP - WLAN interworking user (subscriber) to access service in a serving WLAN different from the home WLAN.

3GPP - WLAN Interworking: Used generically to refer to interworking between the 3GPP system and the WLAN family of standards. Annex B includes examples of WLAN Radio Network Technologies.

(U)SIM Applications/Data: We refer to those applications and data on the (U)SIM that have some security requirements and hence are within the scope of this document.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

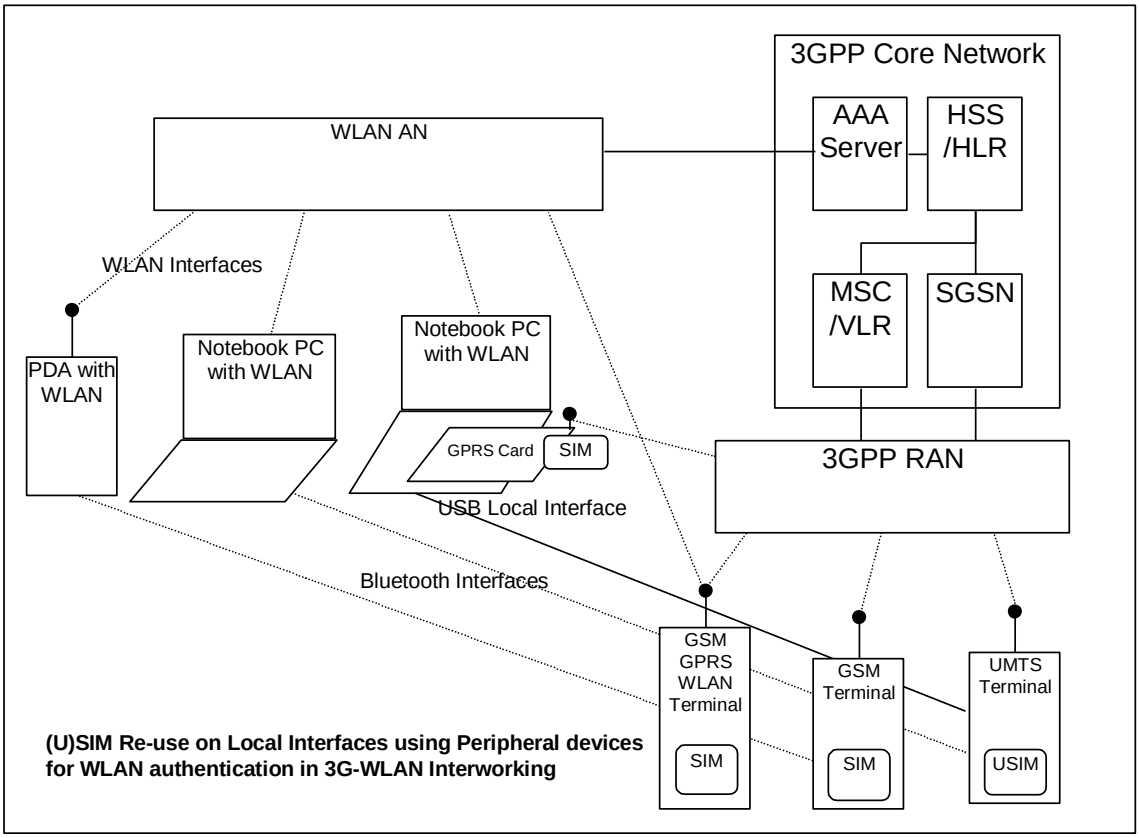
BT	Bluetooth
ME	Mobile Equipment
MT	Mobile Terminal
PC	Personal Computer
PDA	Personal Digital Assistant
SIM	Subscriber Identity Module
TE	Terminal Equipment
UE	User Equipment
USIM	Universal Subscriber Identity Module
IMEI	International Mobile Equipment Identifier
AN	Access Network
RAN	Radio Access Network
PAN	Personal Area Network

4 General Aspects

4.1 Overview

This technical report deals with cases where the user equipment (UE) combination contains at least one MT and may also contain one or more TEs. Some examples are illustrated below. This illustration is only meant to familiarize with the concepts and not imply any limitations for user equipment.

The 3GPP Core network provides the facilities for common access control and charging for 3GPP Radio access networks (RAN) as well as WLAN access networks (AN) as specified in TR 23.934 [3]. The (U)SIM being the authentication mechanism on the UE, and the several models of UE implementations with varied network access capabilities result in the need for understanding the usage scenarios for (U)SIM security re-use in these situations.



NOTE: The figure shows several different scenarios and does not necessarily mean that all the devices shown in the figure are accessing simultaneously using single (U)SIM.

Figure 1: (U)SIM Security Re-use by Peripheral Devices Using Local Interfaces (USB/BT, etc.)

Figure 1 shows some of the different types of (U)SIM security re-use related usage models that are possible. The local interfaces depicted are either BT based or USB based or PC card interface or also could be based on any other wired or wireless interconnect technology. Some of the scenarios illustrated are:

- PDA with WLAN capability re-using the SIM inside a GSM Terminal over a BT interface;
- Notebook PC with WLAN capability re-using the SIM inside a GSM Terminal over a BT interface;
- Notebook PC with WLAN capability re-using the USIM inside a UMTS Terminal over a BT interface;
- Notebook PC with WLAN capability re-using the SIM from a plug-in GPRS PC card module;
- Notebook PC with WLAN capability re-using a USIM from a UMTS terminal over a USB interface;
- GSM-GPRS-WLAN multi-mode terminal re-using the SIM for authenticating WLAN sessions.

It is possible for the 3GPP network and WLAN network to be active at the same time in the examples illustrated and the (U)SIM security re-use model needs to comprehend this requirement. The scope of the work shall follow these listed high-level requirements:

- the UICC is always completely contained in one UE. Furthermore the UICC applications belonging to one subscription are not split amongst multiple UICC or devices;
- network access security shall not be weakened by allowing peripheral devices to access a UICC. Furthermore the security of personal data held on the UICC is not compromised;
- it shall be possible for the operator to charge for access.

4.2 Background and Benefits

The addition of WLANs in parallel to the existing cellular networks is very attractive for cellular operators and it will become more attractive if both the networks interwork together. The simplest interworking scenario would be the common platform for authentication and authorization of subscribers i.e. the user once subscribed with cellular operator would be able to use both cellular as well as WLAN services (provided by the same operator). For this scenario the users may have three options:

1) they must be allotted as many (U)SIMs as many devices they possess;
2) they must be allotted a single (U)SIM removing and inserting the same (U)SIM from one device into another;
3) they can re-use the (U)SIM from an ME or peripheral device using local interfaces.

Both options 1) and 2) have drawbacks. e.g. for option 1), both the user and the operator must bear the cost and inconvenience of getting/handing out additional (U)SIMs. For option 2), only one device can be used to access the network at one time.

Reuse of (U)SIM security by peripheral devices on local interfaces that represents the third option, lacks the drawbacks of options No. 1 and No. 2, and will also offer the following advantages in addition to the above noted merits:

- offers 3GPP system based access control that is a prerequisite for usage of the WLAN-3G interworking service;
- maximize the ease of authentication onto multiple networks that are available to the user;
- allow integrated customer care, which allows for a simplified service offering from both the operator and the subscriber's perspective;
- preserve the support for roaming and session continuity in future;
- evolution of applications without changing hardware or firmware. This will improve service roll-out;
- integration of 3GPP applications with a user's other business, entertainment and communications tools;
- taking advantage of the physical characteristics of personal computers for 3GPP applications (e.g. large display, memory, processing power, etc.).

The goal of this report is to identify usage models related to (U)SIM security reuse. The models should:

- depict outstanding business opportunities;
- be simple enough to allow requirements be captured and technical specifications to be completed in time for Release 6;
- uphold other standards (e.g. Bluetooth, PC-Card) and common industry practice (e.g. major operating systems) where appropriate;
- allow identification of the security issues to be addressed.

Editor's Note: Subscribers certificates can be explored as an alternative or extension to permit the (U)SIM re-use type functionality.

4.3 Related Use Cases

Use-case description: in-car communication

Prerequisites:

The car is equipped with a telematics box containing a MT function.

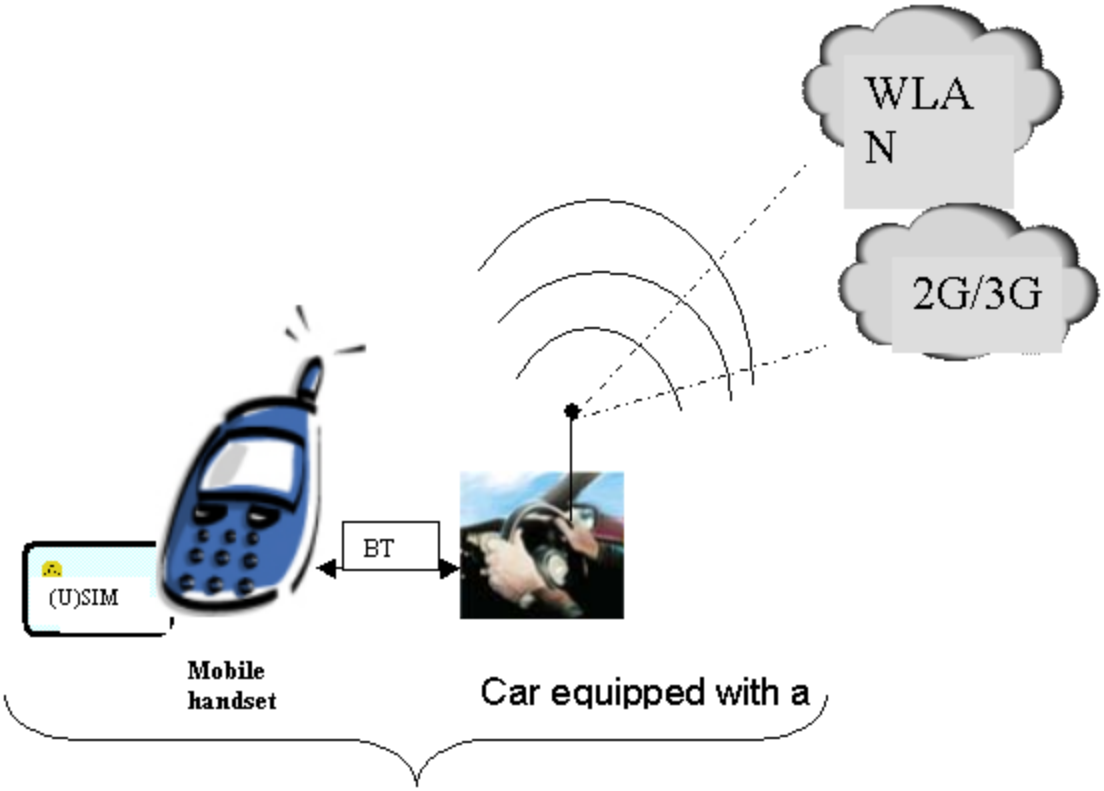


Figure 2: In-car User Equipment for 3GPP and/or WLAN access networks

This figure corresponds to figure 1.

The user has a GSM terminal with SIM, or a UMTS terminal with USIM.

There is a Bluetooth local interface between the telematics box and the GSM/UMTS terminal.

User experience:

The 3GPP subscriber uses the telematics box to access 3GPP and/or WLAN networks. The user authentication is performed by means of the (U)SIM present in the user's GSM/UMTS terminal.

Advantages:

The (U)SIM reuse corresponding to this automotive use-case:

- enables communication from the car to environment;
- facilitates the use of 3GPP services in a car;
- provides a means of user authentication that enables to propose new in-car services (personalized services, DRM in the car, payment, …);
- improves the in-car phone call safety (hands-free call);
- simple for the end-user.

Use case description: Support of TEs

Extending the scope of the subscriber certificates outside the cellular domain to SIMless terminals adds a wide variety of new use cases. Non-cellular terminal support is essential for several alternative access authentication cases where laptop or PC is more convenient terminal than a cellular handset. This section is also relevant for SA3 WI "Feasibility study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces".

The cellular terminal can support usage of bootstrapping or subscriber certificates in SIMless terminal in many different ways. The following four cases are identified:

a. the bootstrapping procedure is done by MT. TE generates Key pair and sends PKCS#10 certificate request to MT. MT authenticates the certificate request on behalf of TE, and then gives the received subscriber certificate back to TE;

b. PTP type of operation according to MeT specifications, i.e. keys and certificate are stored in MT, and TE request MT to perform needed actions using PTP protocol. [MeT] key pair in MT. TE uses the certificate and key-pair stored in MT for operations. The transfer is via local links such as Bluetooth, cable, and Infrared etc.;

c. MT provides bootstrapping interface to TE, therefore it is the TE who triggers bootstrapping procedure. Bootstrapping keys would stay in MT but TE could request MT to do operations by using those keys. In this case, the TE does certificate request since key-pair is generated in TE (or use other NAFs), yet the MT shall authenticate the request on behalf of the TE;

d. MT does bootstrapping, then MT gives the shared keys to TE, and TE does certificate request as well as the authentication of the request.

The 4 cases are aimed to achieve similar functions yet taking slightly different approaches. The detailed explanation is given in following sections.

4.3.1 Case 1

Case 1 is illustrated in figure 3. There are 4 messages in the figure.

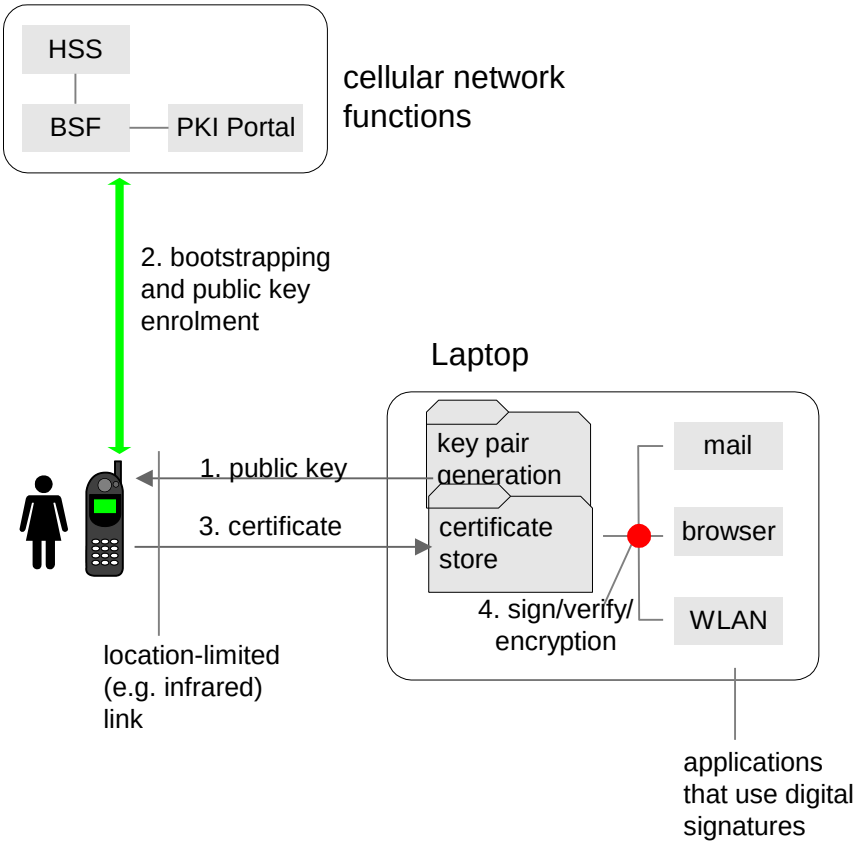


Figure 3: Illustration of case 1.
The public key is transferred from user's laptop to the phone over location-limited link and then certified by the cellular network

In step 1 a public key is transferred from user's laptop to the mobile phone over location-limited (e.g. infrared, bluetooth) channel. The user's key pair may be in a laptop, or in a smart card connected to the laptop's smart card reader.

In step 2 the phone performs bootstrapping procedure with the cellular network and obtains a certificate for user's public key. The user must authorize this operation, for example, by entering a PIN into her phone.

In step 3 the certificate is transferred back to the laptop and installed in laptop's certificate store or into user's smart card.

In step 4 applications use the certified key pair for any of signing, verification and encryption purposes. If operator CA's certificate is also obtained in step 2 and installed to the laptop, or smart card in step 3, applications may use it when verifying digital signatures in step 4. This also enables mutual authentication.

4.3.2 Case 2

Case 2 is illustrated in figure 4. There are 4 messages in the figure.

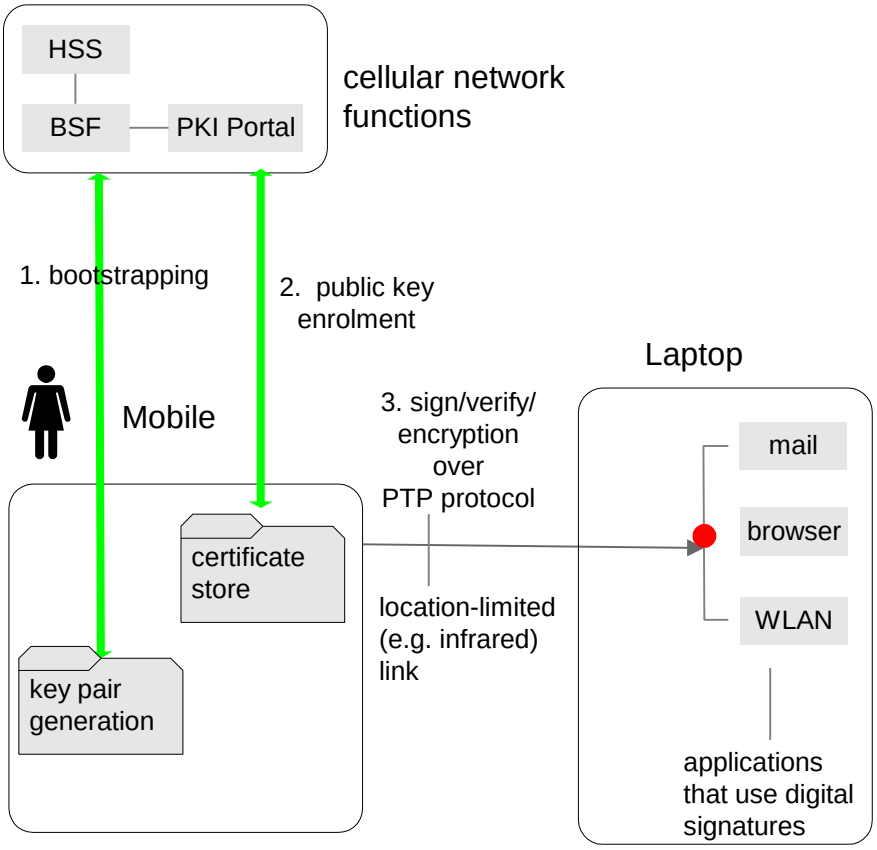


Figure 4: Illustration of case 2.
The public key is transferred from user's laptop to the phone over location-limited link and then certified by the cellular network

In step 1 the User's mobile phone shall trigger the bootstrapping procedure. The user's key pair are generated in the mobile phone, or in a smart card inserted in the phone.

In step 2 the phone performs the certificate enrolment for user's public key. This is in line with procedure specified in TS 33.221 [14].

In step 3 applications use the certified key pair for any of signing, verification and encryption purposes. If operator CA's certificate is also obtained in step 2 and installed to the laptop, or smart card in step 2, applications may use it when verifying digital signatures in step 3. All the transactions over the local link are done over MeT PTP protocol [12] in this flow.

4.3.3 Case 3

Case 3 is illustrated in figure 5. There are 4 messages in the figure.

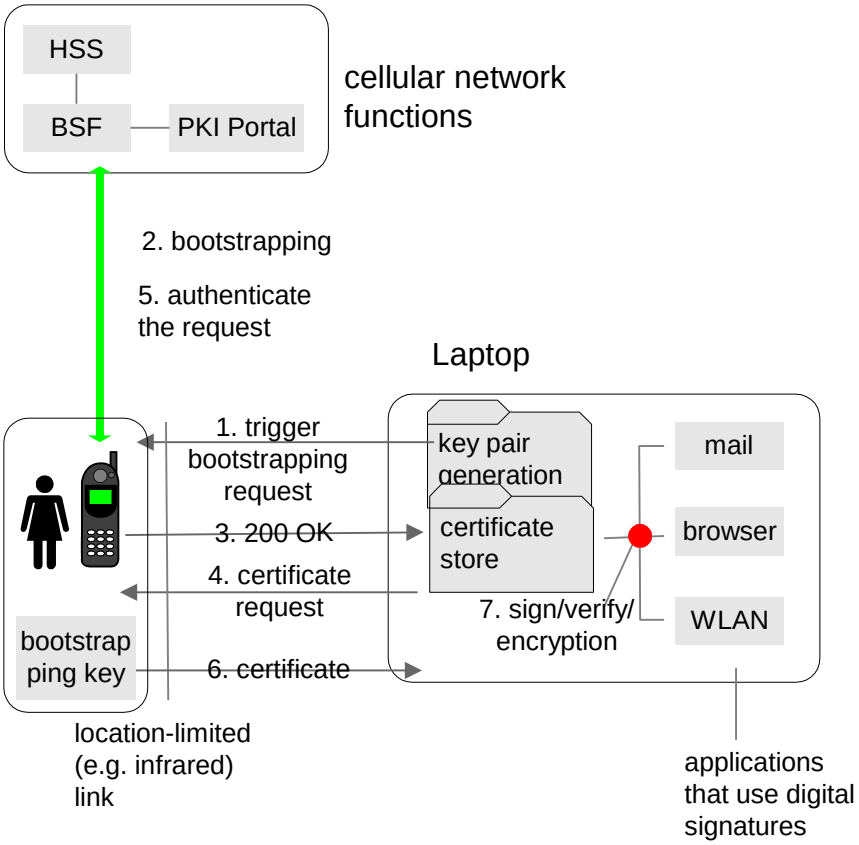


Figure 5: Illustration of case 3.
The laptop triggers bootstrapping procedure as well as the certificate request

In step 1 the laptop shall trigger the bootstrapping procedure. The user's key pair may be in a laptop, or in a smart card connected to the laptop's smart card reader.

In step 2 the phone performs bootstrapping. This is in line with TS 33.220 [13]. And in step 3 the phone acknowledges the success of the procedure.

In step 4 the laptop triggers the certificate enrolment. And in step 5 the phone authenticates the certificate request towards to PKI portal. In step 6, the certificate is transferred back to the laptop and installed in laptop's certificate store or into user's smart card. Step 6 here is identical as the step 3 in case 1.

Finally, in step 7, applications use the certified key pair for any of signing, verification and encryption purposes. This is identical as the step 4 in case 1.

4.3.4 Case 4

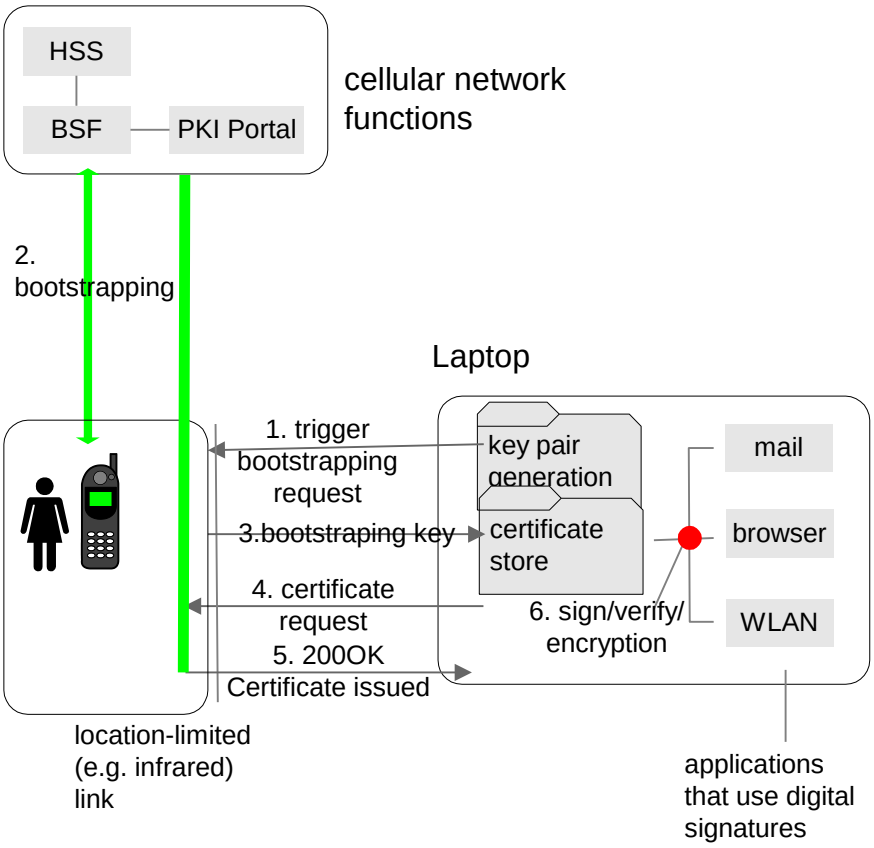


Figure 6: Illustration of case 4.

In step 1 the laptop shall trigger the bootstrapping procedure. The user's key pair may be in a laptop, or in a smart card connected to the laptop's smart card reader. In step 2 the phone performs bootstrapping. This is in line with TS 33.220 [13]. Step 1-2 are identical as that in case 3.

And in step 3 the phone acknowledges the success of the procedure, and also transfer the key generated for certificate request to the laptop.

In step 4 the laptop triggers the certificate enrolment. And in step 5 the certificate is issued. Since the laptop has the key, the request is authenticated by laptop itself; mobile simply transparently forwards the messages.

Finally in step 6, applications use the certified key pair for any of signing, verification and encryption purposes.

4.4 Issues to be addressed

The current specifications of SIM and USIM in 3GPP assume a one-to-one association between the UICC and the Mobile Equipment (ME) to constitute the User Equipment (UE). While this assumption holds in many situations it does not hold for many of the examples illustrated in figure 3, especially in the context of WLAN. This section attempts to capture some of the important issues that need to be addressed for making (U)SIM re-use feasible for the usage scenarios illustrated in figure 3.

For these diverse usage models the specific security threats and issues need to be studied and appropriate security requirements need to be specified to counteract the threats. Following are some security related issues:

- **Issue 1**: The (U)SIM authentication process once it is complete, the key setting procedure that takes place assumes further use of the same radio interface, namely GSM, GPRS or 3G. For the case of GPRS the Kc and CKSN are saved on the SIM for the subsequent authentications. For the 3G case, the CK and IK are saved for subsequent authentications also.

- **Issue 2:** The ME that needs to check the presence of the (U)SIM may not be effectively able to do that as is done today for 3GPP terminals when the (U)SIM is re-used for WLAN authentication over a BT link. The Bluetooth link, if for some reason encounters some interference that prevents SIM presence detection, the WLAN session authenticated using the local link will have to be dropped.

- **Issue 3**: If Pseudonyms are used for Identity privacy as specified in EAP-SIM and EAP-AKA protocols they could be stored on the SIM and USIM respectively or on the ME. This may require additional specification for secure storage.

- **Issue 4**: The SIM and USIM user authentication (PIN entry based) that is performed for the native GPRS/GSM or 3GPP system use and also will be needed for the WLAN use for better protection. This may require additional specification and modifications to the (U)SIM or security architecture specifications.

- **Issue 5**. How many and which kind of UE's should be allowed to have simultaneous access and should the number of UE's be visible to operators?

- **Issue 6**. Which degree of control does the device holding the (U)SIM require on the type of operations that other devices perform with its (U)SIM?

NOTE: Related to issues 1, 3, and 4: The SIM specification was frozen at Rel-4 and cannot be changed. If any other information (e.g. keys or pseudonyms) is deemed useful to be stored on the UICC, new fields need to be specified. These fields are expected to be both device- and access-specific (e.g. stored WLAN keys are not useful for 3GPP access).

4.4.1 Issue No. 1

This issue is related to the key setting procedure where temporal keys are derived after the GSM AKA and UMTS authentication processes and they are saved on the (U)SIM. The assumption here is that a subsequent authentication also occurs on the same radio interface. This assumption need not hold true, because the subsequent authentication can occur over WLAN for instance, using the EAP-SIM or EAP-AKA protocols.

Thus the key setting procedure needs to be re-evaluated for its applicability when interleaved radio interfaces of different security levels are used. Also the temporal keys for the WLAN authentication protocols based on EAP-SIM are not the same as GSM.

4.4.2 Issue No. 2

3GPP TS 51.011 on "SIM-ME Interface" requires a mechanism, to ensure that the SIM has not been removed during a card session. Thus ME issues a STATUS command every 30 seconds to detect the inactivity on the SIM-ME interface during a call. If no response data is received to this STATUS command, then the call is terminated within 5 seconds after the STATUS command has been sent.

The issue here is that Bluetooth radio link may encounter severe interference. The level of this noise may be sufficient to interfere with or block an incoming Bluetooth signal. This will prevent SIM presence detection, resulting ongoing WLAN session to drop.

The investigation shows that interference may arise from the sources like 802.11b network, cellular network, or electrical appliances like microwave oven. The analysis given in annex A leads to the conclusion that the result of increasing levels of interference is almost always confined to a slowing of the data rate as more packets need to be resent. Thus consequences of increasing levels of interference in this application are not so severe, and even for the worst-case scenario the issue can be addressed quite easily by enhancing the timer setting for STATUS command for peripheral devices communicating on Bluetooth. The conclusion is further supported by some additional facts listed in annex A

4.4.3 Issue No. 3

This issue can be broken down into the following three parts.

1) Where do we store Pseudonyms used for Identity Privacy as specified in EAP-SIM and EAP-AKA?

2) Do we need to worry about temporary identifiers for the local communications (e.g. Bluetooth ID's)?

3) Do we need any other information stored for this service?

Pseudonyms and other IDs can be stored in a "normal" file on the peripheral devices. This information is not overly sensitive, and is not intended to be hidden from the subscriber. It may be guarded somewhat to prevent accidental erasure, but more security than that doesn't seem to be justified.

Bluetooth has extensive support for service discovery and device IDs. Bluetooth doesn't define a service discovery protocol itself, but offers such services as "getRemDevNam" (Get Remote Device Name). Additional names should not be needed.

There may need to be information stored on the peripheral devices other than the identifiers. These should be of an "installation" time nature (for instance, an icon be placed in the system tray when the link is active) and can be based on a combination of information from the handset (or "server" device) and user input.

If a pseudonym used for identification in the radio access network is transferred between the device holding the (U)SIM and the device with the radio interface, it will be protected according to the requirements on the local interface in section 6.

4.4.4 Issue No. 4

The (U)SIM provides the ability to have a Universal PIN for the card. Now these are specified in the context of SIM, USIM and other 3GPP applications that are on the UICC. However presently there are no separate WLAN related subscription parameters or authentication data that is stored on the UICC. There is a need to specify WLAN related subscription parameters and also authentication data and configuration parameters on the UICC.

Especially in the context of WLAN, the EAP-SIM protocol needs to validate the multiple challenges it receives in terms of using 2-3 triplets (RAND, SRES, Kc). The basic validation that is required is whether the RANDs in all the challenges are unique. This also has to be verified across authentications if possible.

So it is necessary to conceive that WLAN related parameters also need to be protected under the same PIN or a separate PIN should be provided in case the Universal PIN is not used.

4.4.5 Issue No. 5

This issue is related to fraud detection and avoidance. Fraud detection in currently deployed solutions allows subscription inhibition after detection of suspicious events. These events are usually monitored at fixed time intervals, down to a near real-time granularity. Fraud avoidance would have to authorise each new network access request in real time, according to a network operator's access policy. This authorisation decision needs to be based on knowledge of all currently active accesses for the same IMSI. Such simultaneous access scenarios for WLAN are still under discussion in SA1 and SA2. Therefore, impact of (U)SIM security reuse on fraud detection will be evaluated below.

According to section 6, the following fraud scenarios are possible, and somehow related to (U)SIM security reuse:

F1. Impersonation of the subscriber by local attackers, who gained access to the (U)SIM via the external interface.

F2. Impersonation of the subscriber by remote attackers, who gained access to the (U)SIM via Trojan Horse software.

F3. A fraudulent user, sharing his (possibly temporary) flat rate subscription with others via the external interface.

It is the goal of the TS following this TR to avoid fraud scenario F1. However, F1 is still possible because a network operator has no control of a subscriber's local interface configuration. Scenario F2 is generally possible, independent from (U)SIM security reuse. The risk can be reduced by secure device configuration, possibly including additional software like personal firewalls and virus scanners. However, (U)SIM security reuse may increase a subscriber's exposure, because it is sufficient to break one of the devices in a trusted local environment. Vulnerabilities of all devices sum up. F3 is very simple in legacy password-based WLANs. It is much more difficult with (U)SIM-based authentication. With introduction of (U)SIM security reuse, this scenario again becomes very simple. The fraudulent user can just invite other users' devices into his trusted environment to re-use his (U)SIM.

Fraud detection evaluates the following information:

- IMSI
- IMEI
- Serving Network
- Location
- Time
- Charge
- Access Domain

Countering F1 and F3 by limiting the number of simultaneously accessing devices:

Identifying the UE by requesting its IMEI is not possible with WLAN UEs (the MAC address is no substitute for the IMEI). Lack of an IMEI in each UE makes it nearly impossible for a home network to check the number of UEs that request simultaneous network access based on the same (U)SIM. It could be possible to limit the number of PDP contexts or the number of IP addresses related to an IMSI at the same time. (It is currently under discussion to re-use the idea of PDP contexts for WLAN interworking).

Countering F2 by checking device locations:

F2 could be easily detected for GSM, GPRS, and 3G system access, because network-based location information is provided. It is FFS, if similar information can be provided by WLAN access networks.

Applications using (U)SIM security

Other potential uses of (U)SIM security, e.g. bootstrapping of security for issuing subscriber certificates, are by design logically independent from the device holding the (U)SIM and its location. This adds another facet to F1 and F2 that will be very difficult to detect.

Countering F3 by suitable charging model:

F3 becomes unattractive for the fraudulent user, if charging is based on traffic volume. However, it may be unacceptable for a network operator to rule out all (temporary) flat-rate charging models.

Editor's Note: In one of the conference calls, it was discussed that every device in 3GPP needs to be known to the network. 3GPP Network knows through IMEI, but in case of WLAN it is not possible. MAC address is also not possible though it is a unique identifier. If we could ask IEEE?

4.4.6 Issue No. 6

Main focus of Security Reuse is AKA. Reuse of SIM/UICC functions beyond AKA via local interfaces may not be sensible or desirable in every case and must be further studied. Furthermore, the user may wish to restrict access to certain functions or data, e.g. private information in the phonebook.

Another problem may arise due to the fact that the (U)SIM has no possibility to identify or authenticate the device which "talks" to it. Most (if not all) functions were designed with a physical 1:1 relation in mind. One example is the (U)SIM Application Toolkit, which interacts with the I/O facilities of the ME holding it. Problems may arise when (U)SAT functions can be initiated externally via local interfaces but the resulting responses trigger actions on the device holding the (U)SIM.

5 Threat Analysis

This section attempts to capture the security threats involved in the (U)SIM Security Re-use usage models mentioned in this document. The focus is mostly on the vulnerabilities and the threat implications on the (U)SIM authentication data and related aspects when these usage models are in practice. Its important to also note that some of these vulnerabilities and threats have potentially broader implications, but we primarily restrict our discussion to those that are in scope of the document.

Some of the vulnerabilities associated with these usage models are described first and subsequently the resulting threats (specific attacks) that can be realized are analyzed. Its important to note that these threats are applicable to re-use of (U)SIMs both when used remotely from or also on the same equipment when the device has open programmable software environments.

5.1 Environment

The GSM and UMTS networks use licensed/regulated bands and therefore when attackers deploy equipment for performing attacks over the wire it maybe slightly easier to apprehend them by virtue of their using licensed/regulated bands in an illegal manner.

In WLAN as the radio bands are un-licensed, even though still regulated in some countries, the attacker can legitimately deploy attacking equipment and the burden lies on proving the attack related actions being illegal and could require additional efforts.

Also, in GSM/UMTS, the base station equipment may not be as inexpensive as the WLAN access points that are available in the market today. So the likelihood of attacks in WLAN is slightly more significant.

It is also important to note that GSM phones with no or minimal application download capabilities are considered closed or more secure environments as opposed to Laptops and PDAs with broad application download capabilities. The vulnerabilities and resulting threats are analyzed with these assumptions regarding the environment in context.

5.2 Vulnerabilities

The following are some of the vulnerabilities associated with the (U) SIM Re-use usage models.

5.2.1 Exposure of SIM/USIM authentication data

For GSM 11.11 type of interfaces, the SRES and Kc cryptographic parameters are transferred from the SIM to the ME, as part of the GSM AKA protocol. Exposure of these parameters to an attacker is a serious problem that can lead to fraud. For WLAN authentication using EAP-SIM protocol also, these parameters will be used by legitimate devices, but shall not be exposed as the security is based on secrecy of these parameters.

For UMTS USIM type of interfaces the RES, CK and IK parameters are transferred from the USIM to the ME, as part of the AKA protocol. Exposure of these parameters to an attacker is a serious problem that can also lead to fraud. Similarly for WLAN authentication using EAP-AKA protocol also, these parameters will be used by legitimate devices, but shall not be exposed as the security is based on secrecy of these parameters.

It is important to note that GSM/UMTS UEs that have no application download capability maybe able to provide a relatively secure environment where these parameters are protected. But today, as we see more of the application-download capable UEs, additional protection mechanisms maybe needed. Now when (U)SIM is being used directly or re-used to authenticate open mobile platforms like Laptop PCs and PDAs, the protection of these parameters become even more necessary as the likelihood of threats is much higher. This is especially true when 3GPP is considering the SIM and USIM based authentication for WLAN terminals.

5.2.2 Unlimited Invocations of RUN GSM algorithm

The SIM/USIM as they are accessible to all applications on the ME, so if a malicious application is present; it could make unlimited invocations of the RUN GSM algorithm. In the case of the SIM, this may result in the Authentication Counter reaching its limit and the Card locking up, or it could also result in the secret key Ki being revealed in some cases where the algorithms are weak.

In the case of the USIM this may not be a problem as the challenges are also authenticated. The USIM also has the capability to reject challenges when its sequence numbers don't match.

5.2.3 SIM Challenge Freshness

As the GSM AKA is one-way authentication, there could be replay attacks using known RAND challenges that can cause an ME to connect to an un-authorized attacker impersonating the network. On a local interface where the SIM is being re-used for authentication over a WLAN network, there is an increased likelihood of an attack that will try to exploit this vulnerability.

Fortunately, the EAP-SIM protocol for WLAN provides mutual authentication, but as it is essentially based on the GSM AKA protocol at the terminations (UICC end and the AuC/HLR end), it is still possible to perform a successful Network Impersonation attack if known RAND challenges and their responses (SRES and Kc) are obtained. The likelihood of getting such triplets from the network is fairly low, but exposing them on Laptops and PDAs, which are considered open platforms, is more probable.

The USIM does not suffer from such a weakness as it supports full mutual authentication and validates RAND challenge freshness.

However in certain situations when the AuC is unreachable to obtain new triplets or quintuplets, its possible for these to be re-used by the VLR and SGSN respectively. In such situations however they are more likely again to be exposed as result of the UE platforms being more open only.

5.2.4 Eavesdropping

The lack of confidentiality for authentication data on the SIM-ME and USIM-ME interfaces lead to un-authorized applications being able to view the authentication traffic and either re-route it for performing off-line attacks on the secrets or for performing man-in-the-middle type of attacks.

When the SIM/USIM re-use involves, local interfaces like Bluetooth, such eavesdropping could be a serious vulnerability if the default Bluetooth security that is known to be weak is compromised.

5.2.5 Lack of WLAN terminal authentication

The SIM/USIM when it is used for WLAN authentication, there is no concept of IMEI that validates that the terminal is authorized for use on the GSM operator WLAN network. Hence the SIM/USIM used for authentication could be from a stolen subscription and there is no direct way of verifying that. The CHV(PIN) on the SIM/USIM card provides some degree of protection if enabled, but often it seems to be disabled by users and hence is a security risk. Also it is necessary to distinguish the situations of honest lending versus when identifying a terminal's use of the network.

5.2.6 Lack of Identity Privacy

The IMSI, which is the permanent identity, can be forced to be revealed by malicious applications on the ME, which could result in the privacy being compromised.

5.3 Threats

The following are some of the attacks that are possible due to the vulnerabilities identified in the previous section. The attacks described here are mostly restricted to those that are possible on local interfaces. Some of the threats below are not new, but today attacks require physical access to the card or to the (U)SIM-ME interface. This implies theft of the UE or cooperation of the subscriber. Security Reuse via a wireless local interface no longer requires physical access for these attacks, which justifies cryptographic security measures.

5.3.1 Attacks on the SIM secret

The unlimited calls to RUN GSM could be used to attempt cracking the SIM secret. It is known that when COMP-128-1 based algorithms are in use, this is actually a feasible attack if the authentication counter is not enabled.

5.3.2 Man-in-the-middle/Connection Hijack attacks

The (U)SIM-ME interface is utilized to perform authentication on behalf of another terminal that is not authorized to use the (U)SIM, then a man-in-the-middle (Mitm) attack results, where the Mitm steals authentication state and thus is able to successfully obtain access to the network fraudulently.

5.3.3 Impersonation of a subscriber

The (U)SIM-ME interface is utilized to perform authentication on behalf of another terminal. This attack can be used successfully with SIM and USIM based WLAN authentication.

5.3.4 Impersonation of the network

As the SIM authentication is one-way and no freshness of the RANDOM challenges is enforced, it is possible for compromised triplets (RAND, SRES, Kc) to be used for impersonating a valid network when being used for WLAN authentication.

6 Potential Requirements

According to the proposal, "(U)SIM Security Reuse by Peripheral Devices on Local Interfaces" the (U)SIM card may reside in a 3GPP UE and be accessed by a WLAN-UE through Bluetooth, IR or a USB cable or some other similar wired or wireless interconnect technology. This would facilitate the user to get simultaneous WLAN and 3GPP access with the same (U)SIM. In order to accomplish this, while at the same time addressing the issues and threats mentioned above, following requirements shall be satisfied:

R1. A secured interface between the device holding the (U)SIM and the device with the radio interface is required. This interface must be able to protect against eavesdropping, and undetected modification attacks on security-related signalling data (e.g. authentication challenges and responses). Cryptographic or physical means may be used for this purpose.

R2. For cryptographic means, the encryption key length shall be at least 128 bits.

R3. Keys used for local interface transport security should not be shared across local interface links. Each local interface must 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).

R4. Both endpoints of the local interface shall be mutually authenticated and authorized.

R5. The device without (U)SIM should be capable of discovering the device(s) with (U)SIM in its proximity.

R6. 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 remote (U)SIM, e.g. to reset it, or to switch its power on or off.

R7. 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 also has the ability to terminate an authenticated network sessions when, the (U)SIM is no longer accessible within a short monitoring time period.

R8. User shall have the capability to shut off sharing of (U)SIM feature. The owner of the device, holding the (U)SIM should authorize its use.

R9. 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 should be guarded against.

R10. Whenever someone tries to remotely access a (U)SIM some sort of alert may be sent, e.g. a message will be displayed informing the user of the access. The user can then decide whether the access is authorized and can allow or disallow it. The security level must 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.

R11. It shall be possible to simultaneously access both WLAN and 3GPP radio access technologies, i.e. it should 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.

R12. The UICC bearing device should be responsible for serializing access to the (U)SIM Application/Data.

R13. The user should be able to select (U)SIM and TEs as part of their user equipment combination.

R14. A standardized API for access to capabilities provided by an MT (TE) towards a TE (MT) across Operating Systems must be provided.

R15. UICC presence detection shall be supported via the local interface. The local interface may need to address Issue No. 2, e.g. by retransmission of the STATUS command.

R16. Security Reuse shall be consistent with current security arrangements for Release 6 and ensure that user security is not compromised.

R17. 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 should be applied by the 3GPP ME bearing the (U)SIM.

NOTE: This access control, related to Issue No. 6, is ffs.

6.1 Potential Link-specific Requirements

6.1.1 Potential Requirements for Bluetooth

With the SIM Access Profile, Bluetooth SIG specified functions which meets some of the requirements for Security Reuse. However, some requirements must 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 at least one additional device to access the card concurrently (R12).
2. Access to SIM, USIM, and ISIM shall be possible.
3. The local interface may need to provide integrity protection (R9, R16).

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. Mandatory security requirements for the pairing must be specified to be enforced by the ME. This will ensure local interface security (R1, R16). Users may not be aware of the fact that a short PIN does not provide adequate protection against brute-force attacks.

NOTE: This list may not be exhaustive.

6.1.2 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, IR, 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 should always be set to "Do Not Auto Connect" or "Do Not Make Discoverable".

   The user must 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 should be no "auto-accept" feature on the device).

   The requesting device should represent itself via its Unique Identifier.

3. **Unique Identifier**

   The user should 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 should only be enabled after the user provides a Unique Identifier.

4. **Password Change**

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

5. **Access Level Controls**

   The user should 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.

7 Feasibility of diverse usage models

7.1 Security Architecture Proposal

Figure 7 identifies the function required for (U)SIM security reuse in the context of the components described in TS 24.002 [10]. (U)SIM security reuse requires a new TE function (hatched) that implements the external Cc interface, security functions, and user interface additions identified in this document. Depending on the physical layer, the external Cc interface can have a PAN structure, i.e. support many-to-many relations.

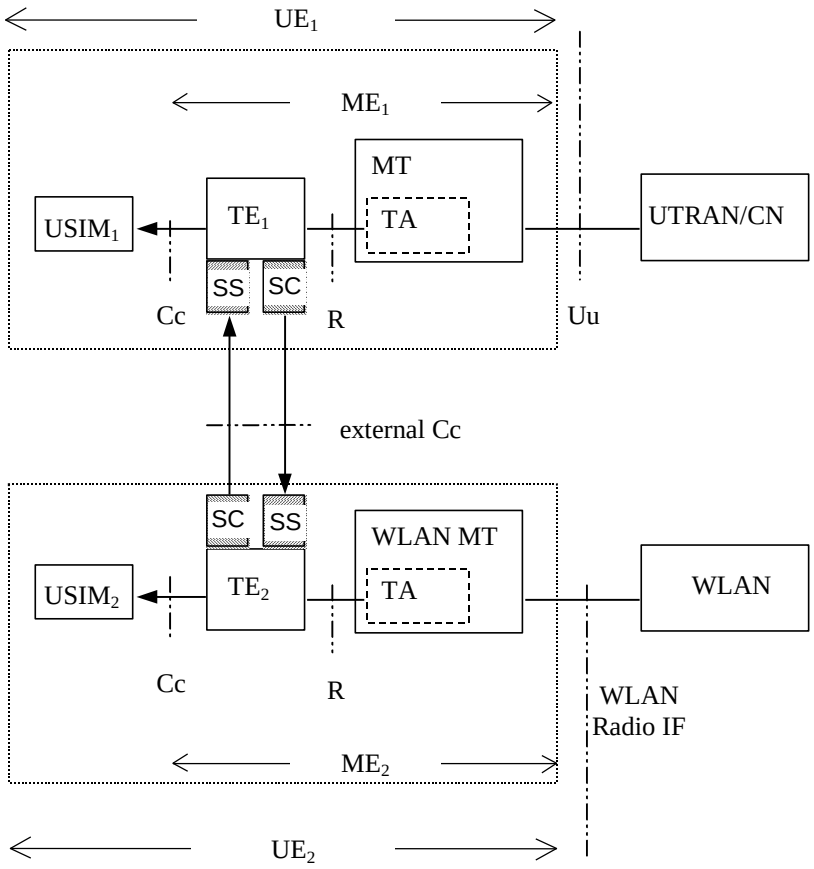


Figure 7: Security Architecture Reference Model

To give an example: In figure 7, the components could be implemented as follows:

UE1: Mobile phone with TE1 being its CPU, and MT integrated.

UE2: Laptop (TE2) with an integrated smart card reader (Cc interface) and a PCMCIA (R interface) WLAN card.

The external Cc interface has two functional aspects: A security server (SS) forwards security functions provided by a local (U)SIM to external devices, and a security client (SC) which makes use of functions provided by an external security server.

7.2 Impact on current security specifications

During the feasibility study no impact on any of the 3GPP core network elements has been identified. However, if any impact is realised later, will be addressed accordingly.

7.3 Additional user authentication requirements

7.4 Impact on any 3GPP core network elements

8 Conclusion

TR 22.934 v6.1.0 [3] on 3G-WLAN interworking requires the ability for a (U)SIM to be used for providing common access control and charging for WLAN and 3G services using the 3GPP system infrastructure. The current specifications of (U)SIM assume that User Equipment (UE) has one-to-one association between the UICC and the Mobile Equipment (ME). This assumption does not hold for several diverse usage models.

This TR signifies those usage models, studies the associated issues, analyses specific security threats, and develops appropriate security requirements for the usage models. It also studies the impact on current security specifications for 3GPP, especially with regards to key setting procedures, and USIM sequence number synchronization, UICC and UICC-application presence and detection/UICC application presence detection issues and termination of the UICC usage etc. It also addresses the additional user authentication requirements (e.g. PINs) and device management requirements when used over local interfaces such as Bluetooth, IR or USB. The TR also examines the impact on 3GPP core network elements.

8.1 Recommendations

The feasibility study has examined the (U)SIM Security Reuse by Peripheral Devices on Local Interfaces for Rel-6. The essence of the proposal is that the (U)SIM card resides in a 3GPP UE and be accessed by a WLAN-UE through Bluetooth. This would facilitate the user to get simultaneous access on WLAN and 3GPP networks with the same (U)SIM.

The Feasibility Study has scrutinized and proposed solutions to the various issues that were raised during this study. It has identified requirements, performed threat analysis, developed a preliminary Security Architecture Reference Model, and catalogued a list of the impacted TSs. No over-riding issues remain. Hence it is recommended that the result of this feasibility study may either be incorporated in TS 33.234 [4] Wireless Local Area Network (WLAN) Interworking Security (Release 6) or other existing TSs, or WID and TS should be started with enhanced scope to address the following additional recommendations.

Additional Recommendations:

R1. Based on (U)SIM Re-use, Security Architecture may be developed further.

R2. The SIM specification is frozen at Rel-4. If the usage models (presented in the TR or to be studied in future) are deemed useful, (U)SIM security re-use may be enhanced to include SIM as well.

R3. We need to further study the need to specify WLAN-related subscription parameters and also authentication data and configuration parameters on the UICC. SA3 needs to specify WLAN related subscription parameters and also authentication data and configuration parameters on the UICC for:

- the WLAN-UE Functional Split case in WLAN interworking. This is a specific application of the principles of (U)SIM Security Re-use on Local Interfaces;
- the non-WLAN-UE Functional Split case in WLAN interworking. This is where the WLAN-UE has a traditional interface to its own UICC.

In both cases, SA3 needs to determine the optimal distribution of these parameters between the UICC and the WLAN-UE (or other components in the functional split model) and their persistence, taking account of the following:

- security protection of the parameters in storage and transfer;
- performance when first accessing and moving between networks;
- compatibility with existing WLAN Client software.

R4. Bluetooth Architecture Review Board (BARB) and the Bluetooth Car Working Groups (CWG), may be asked to look into supporting simultaneous access of mobile devices to 3GPP and WLAN networks based on (U)SIM security reuse, either by extending the scope of the existing SIM Access Profile or by developing a new multi-profile architecture.

Annex A:
Additional Information on Issue No. 2

802.11b devices, similar to Bluetooth, operate within the 2.4 GHz band. The difference is that Bluetooth uses frequency hopping (at 1600 hops per second) to hop over the entire 2.4 GHz band. 802.11b, on the other hand, uses direct sequence and only occupies approximately one third of the 2.4 GHz band. As a result, Bluetooth hops all over 802.11b transmissions. Because of the potential for collisions, Bluetooth devices can suffer interference. Most of the research studies show that the result of increasing levels of interference is almost always confined to a slowing of the data rate, as more packets need to be resent. Thus the consequences in this application are not severe. Only in extreme conditions, such as setting a Bluetooth device next to an operating microwave oven, it is likely that communications will cease altogether.

In GSM environment wide-band noise is generated from the GSM internal and spurious radio signal interference (cellular transmitter and radio up-converter). Some of this noise appears in the Bluetooth band. The level of this noise may be sufficient to interfere with or block an incoming Bluetooth signal. However, Bluetooth modules using special radio filters (that does not have a spurious response in the 2.4 GHz band) can be developed and used at the output to combat noise.

The 3G WCDMA systems may also challenge Bluetooth because WCDMA signals (usually 2.1 GHz) are so close to the 2.4 GHz band used by Bluetooth. Though Bluetooth has a well thought-out architecture to survive in this harsh radio environment, yet, testing of real radios is the only way to insure compatible high performance solutions. However, we believe that in this particular application of Bluetooth, i.e. (U)SIM Security Reuse by Peripheral Devices on Local Interfaces, Bluetooth link will be used mainly for authentication only, and the signalling traffic on the link will not be very high (A STATUS command is issued every 30 seconds and call is terminated within 5 seconds after the STATUS command has been sent). Thus even in the face of increasing levels of interference the consequences will not be severe. Furthermore even if interference consequences are found alarming, the timer for STATUS command for peripheral devices can be enhanced.

Finally Bluetooth SIG is also aware of the problem and in conjunction with the IEEE 802.15.2 task group, has been collaborating on efforts to alleviate interference problems under worst-case scenarios. They are defining mechanisms and recommended practices to ensure the coexistence of Bluetooth and Wi-Fi networks. Eventually the practices will likely become part of the standard. These practices are given below.

These practices fall into two categories:

Collaborative mechanisms:

Mechanisms in which the wireless personal area networks (Bluetooth), and the WLAN communicate and collaborate to minimize mutual interference. The following mechanisms ensure reduced interference.

TDMA (Time Division Multiple Access) techniques allow Wi-Fi and Bluetooth to alternate transmissions.

MEHTA is a technique for managing packet transmission requests. It grants permission to transmit a packet based on parameters including signal strength and the difference between 802.11 and Bluetooth centre frequencies.

Deterministic frequency nulling is a mechanism used in conjunction with MEHTA that inserts a 1 MHz-wide null in the 22 MHz-wide 802.11 carrier that coincides with the current Bluetooth centre frequency.

Non-collaborative mechanisms:

Mechanisms in which there is no method for the Bluetooth and WLAN to communicate. Non-collaborative techniques being investigated are:

Adaptive packet selection and scheduling

It is a Bluetooth Media Access Control (MAC)-level enhancement that utilizes a frequency usage table to store statistics on channels that encounter interference. This table can subsequently be accessed by packet scheduling algorithms that schedule transmissions to occur only when a hop to a good channel is made.

Adaptive frequency hopping

Classifies channels and alters the regular hopping sequence to avoid channels with the most interference.

Bluetooth intended to operate in a cellular phone environment may suffer from interference caused by wide-band noise generated by the cellular transmitter and radio up-converter. Some of this noise appears in the Bluetooth band. The level of this noise may be sufficient to interfere with or block an incoming Bluetooth signal.

However, Bluetooth systems using special radio filters can be developed that can combat noise from the GSM internal and spurious radio signal interference. To ensure that the Bluetooth radio module will operate effectively inside a cellular phone, the level of noise from the phone's transmitter must be measured and controlled. This is particularly true if the phone uses a filter at the output. It is important that this filter does not have a spurious response in the 2.4 GHz band.

The 3G WCDMA systems will challenge Bluetooth even further WCDMA signals (usually 2.1 GHz) are so close to the 2.4 GHz band used by Bluetooth. However overall, Bluetooth has an innovative and well thought-out architecture to survive in this harsh radio environment, but extensive testing of real radios is the only way to insure compatible high performance solutions.

Annex B:
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 password from 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 and 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 reference [C.5] with the full details available from reference [C.10].

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.

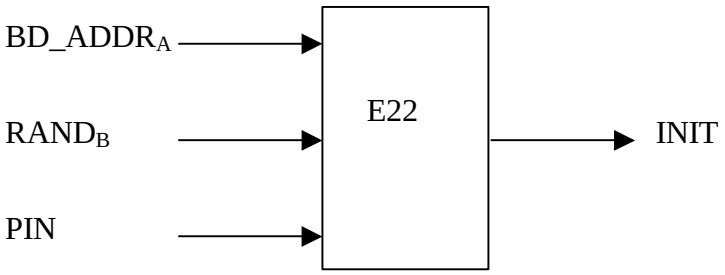


Figure B.1

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:

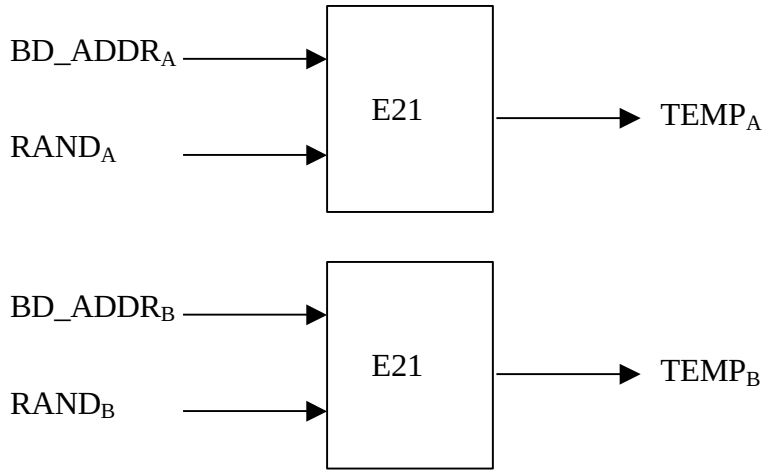
1. A encrypts its unit key with the initialisation key and sends this to B.
2. B decrypts the message with the initialisation key.
3. Both devices now have A's unit key, and they use this as the link key. The initialisation key is now discarded.

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.



$$Temp_A \oplus Temp_B \rightarrow LINK$$

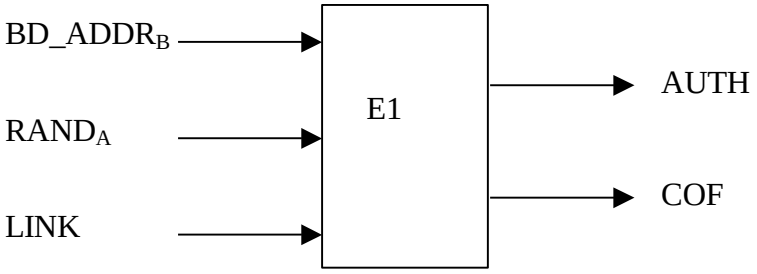
Figure B.2

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.



Figures B.3

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).

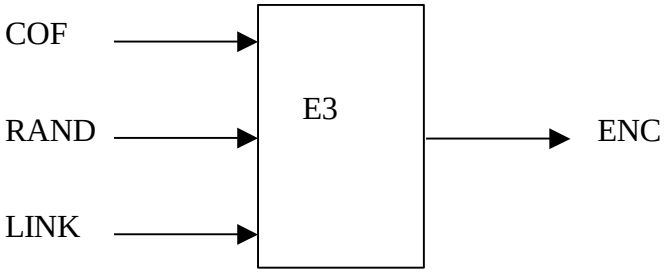


Figure B.4

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

Table B.1

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: [C2] [C3] [C4] [C5] [C6]	
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 [C4] [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

Ref.	Consideration	Recommendation	Remarks
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 μs, so 2^{28} * 312.5 μs = 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: [C6] [C7]	This recommendation has been requested to be adopted as a requirement in the CR on section B.3. See 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)
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: [C6] [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.	A warning should be implemented to inform users about vulnerabilities that are inherent with Bluetooth devices in discoverable mode. c.f. Bluesnarfing and Bluejacking.	This recommendation has been requested to be adopted as a requirement in the CR on section B.3.

Ref.	Consideration	Recommendation	Remarks
	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.	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: [C3] However, non-discoverable mode can also be attacked see concern 6 below.	See section B.3 requirement 4.
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: [C8] [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.3. See section B.3 requirement 5

Annex C: 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".

Annex D:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2004-03	SP-23	SP-040169	-	-	Presented for approval at TSG SA #23	1.1.2	2.0.0
2004-03	SP-23	-	-	-	Approved and placed under Change Control (Rel-6)	2.0.0	6.0.0
2004-12	SP-26	SP-040860	001	2	Bluetooth security and configuration considerations for Annex of TR 33.817	6.0.0	6.1.0
2004-12	SP-26	SP-040860	002	2	Update to not rule out the use of the smart card for security enhancements	6.0.0	6.1.0