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)
Source:	⌘	Toshiba and supporting Companies
Work item code:	⌘	(U)SIM Reuse
Date:	⌘	08/04/2004
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. TS 33.817).
Summary of change:	⌘	Some minor changes mostly the insertion of reference of 33.817 to accommodate the additional feature.
Consequences if not approved:	⌘	New feature could not be supported.

Clauses affected:	⌘	2, 4.1.4, 4.2.4.1, 4.2.4.3, 6.1.1, 6.1.5, C3.1
Other specs affected:	⌘	Y / N [ ] N [ ] N [ ] N
	⌘	
Other comments:	⌘	

***** 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".

***** 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 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:

- 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.

- 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).

- 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.

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

- 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.

- 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].

- 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.

- 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.

- 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.

- 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.

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

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

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

- 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.

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

- 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.

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]. However it shall meet the following:

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 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 at least one additional device to access the card concurrently (Requirement No 12).

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. 16).

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 shall be specified to be enforced by the ME. This will ensure local interface security (Requirement No. 1, Requirement No. 16). 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.

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 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 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[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 *****