3GPP SA Plenary #21
22-25th September 03
Frankfurt, Germany T.Doc. No. SP- 030397

- **Title:-**
  - Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces
- **Source :-**
  - Toshiba, Intel, T-Mobile, Nokia, Telcordia, Thomson, Fujitsu, HP, RIM, SmartTrust, BT Group PLC, Alcatel
- **Contact:-**
  - Raziq Yaqub, Toshiba America Research Inc., (ryaqub@tari.toshiba.com)
- **Agenda item:-**
  - For Release 6
- **Document for:-**
  - Information

Preface

Proposal

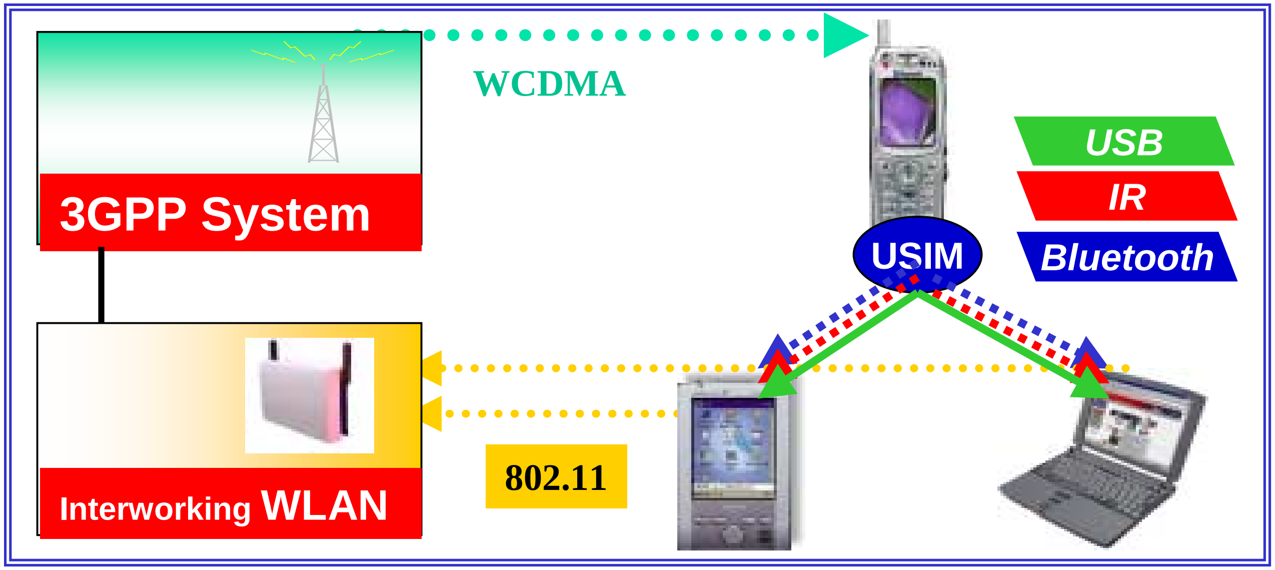
“Feasibility Study on (U)SIM Security Reuse by Peripheral Devices on Local Interfaces”

Essence of the Proposal,

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 technology.

This would facilitate the user

To get simultaneous WLAN and 3GPP access with the same (U)SIM



Introduction

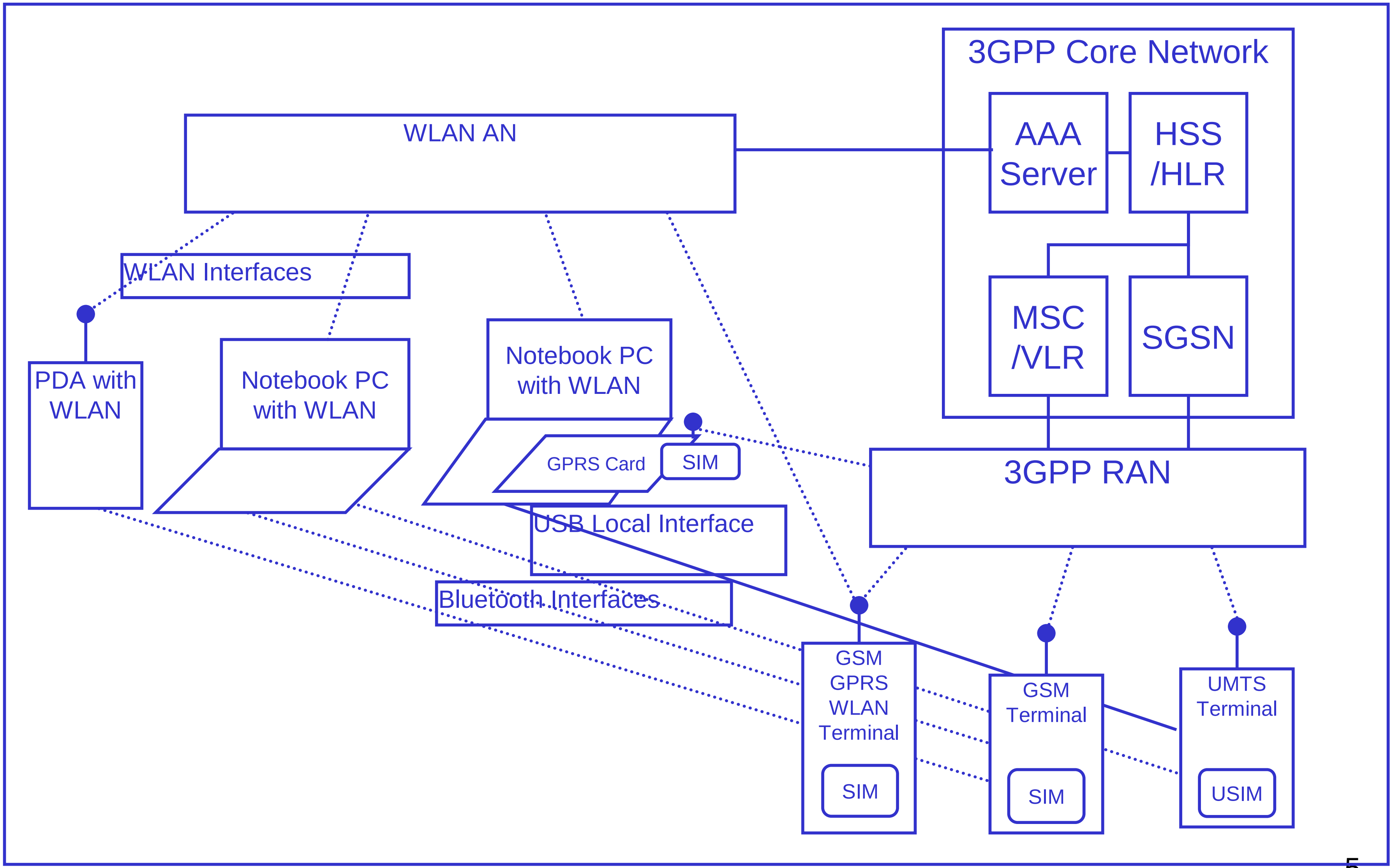
- **Wireless Local Area Networks (WLANs)**
  - Dramatically altering the landscape of wireless data access.
  - Effectively a complementary radio access technology to 3GPP system.
- **Interworking of Public WLAN and 3G**
  - Has become important.
  - Requires common AAA functions using 3GPP infrastructure, i.e.
  - Use (U)SIM for common “access control” & “charging” for W/3G services
- **I-WLAN Usage Models Vs one-to-one Association of UICC & ME**
  - Current specifications assume one-to-one association of UICC & ME
  - Models derived from I-WLAN requirements do not hold this assumption
- **This suggests Studying Reusing (U)SIM Security Local Interfaces.**
  - Including specific security threats and issues
  - Specifying appropriate security requirements

Examples of Diverse Usage Models where one to one association is not possible

- **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

Examples of Diverse Usage Models where one to one association is not possible

(U)SIM Re-use on Local Interfaces using Peripheral devices for WLAN authentication in 3G-WLAN Interworking



Scope of the TR

- **Conduct a Threat Analysis.**
  - To realize diverse usage models from security point of view
  - To study the impact on having many entities using the same security mechanism and 3GPP core network elements
- **Determine the Feasibility of Reuse of a Single (U)SIM by**
  - By peripheral devices
  - On local interfaces to access multiple networks
  - Without incorporating significant changes to 3GPP/WLAN infrastructure.
- **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 Include**
  - 3GPP and WLAN type networks.

Scope of the TR (Contd.)

- **Study the Impact on Current Security Specifications for 3GPP**
  - Key setting procedures,
  - USIM sequence number synchronization,
  - UICC presence detection and termination of the UICC usage etc.
- **Study Additional User Authentication Requirements**
  - (e.g. PINs) when used over local interfaces like Bluetooth, IR or USB.
- **Study the Proposals**
  - To realize the desirable usage models for (U)SIM re-use
- **Make Recommendations**
  - By analysing the trade-offs involved in the impact to the ME and (U)SIM

High Level Issues that Require 3GPP Specification Related work

- **Issue No.1**
  - Presently (U)SIM re-use related security specifications on local interfaces (e.g.BT) for simultaneous access to the (U)SIM do not exist.

Bluetooth SIG SAP could be considered with some potential modifications because it is transport specific, and does not support SIM re-use with multiple accesses over multiple interfaces

- **Issue 2:**
  - SIM Presence detection over local interfaces is not specified.
    - Local interfaces may have link reliability issue

      (e.g., radio interference could cause a WLAN session to be dropped)
    - Local interfaces may have link security issues

      (e.g false presence status could be presented)
- **Issue 3:**
  - If Pseudonyms are used for Identity privacy as specified in EAP-SIM & EAP-AKA protocols, they could be stored on SIM & USIM respectively or on the ME. This may require additional specification for secure storage.

Issues to be Addressed (Contd.)

- **Issue 4:**
  - The SIM & USIM user authentication (PIN entry based that is performed for the native GPRS/GSM or 3GPP system) will also 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.**
  - Which kind of ME’s should be allowed to have simultaneous access
  - How many ME’s should be allowed to have simultaneous access
  - Should the number of ME’s be visible to operators?
- **Security Issues**
  - Specific security threats need to be studied and addressed
  - Security requirements need to be specified to counteract the threats.

Requirements

- **Secured Interface** **[DH(USIM) = Device Holding (USIM), DL(USIM) = Device Lacking (USIM)]**
  - Secured interface between the DH(U)SIM and the DL(U)SIM
  - Mutually authentication/authorization of both endpoints of local interface
  - Usage of unique keys over each local interface for cryptographic means
  - Encryption key length shall be at least 128 bits.
- **(U)SIM Discovery and Communication**
  - Discovery of DH(U)SIM by DL(U)SIM in its proximity.
  - DL(U)SIM shall not change the power on or off status of DH(U)SIM.
  - Termination of sessions when DH(U)SIM is no longer accessible.
- **User's Permission**
  - The owner of the DH(U)SIM should permit/control its use
  - Some alert/message will be displayed informing the user that someone is trying to remotely access (U)SIM. The user can then deny or permit

Requirements (Contd.)

- **Simultaneously Access Both WLAN and 3GPP**
  - Support simultaneous calls on two different air interfaces. For example, WLAN for internet access together with 3GPP system for a speech call.
- **Security Level**
  - Integrity and privacy of signalling between WLAN system and 3GPP CN
  - Same or better security level as of present GSM System or as defined by IETF (EAP-SIM, EAP-AKA)
- **Implementation**
  - User be able to select from multiple (U)SIM in a personal set of UE's as part of his UE combination.
  - A standardized API between the DH(U)SIM and the DL(U)SIM for (U)SIM access across Operating Systems must be provided.

Benefits

- **Ease of Authentication**
  - Maximize the ease of authentication on multiple networks available to user
  - “No Removal/insertion of USIM from one device to another device”.
  - “Simultaneous access to both networks”
- **Integrated Customer Care**
  - Allows simplified service offering from operator/subscriber’s perspective
- **Roaming and Session Continuity**
  - 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**
  - Integrates user’s business, entertainment and communications tools.
- **Takes Advantage of Physical Characteristics of Devices**
  - PC with large display, memory, & processing power for 3GPP applications

Thanks