Technical Specification Group Services and System Aspects **TSGS#17(02)0514**
Meeting #17, Biarritz, France

Source: **SA WG3**

Title: **5 Security WIDs**

Document for: **Approval**

Agenda Item: **7.3.3**

The following WIDs were agreed by SA WG3 at their meeting #24 and are proesented to TSG SA for approval.

S3-020429:	Support of the Presence Service Security Architecture
S3-020430:	3GPP Generic User Profile Security
S3-020432:	Release 6 User Equipment Management: Security aspects
S3-020433:	Security Aspects of Multimedia Broadcast/Multicast Service (MBMS)
S3-020451:	WLAN Interworking Security WID

3GPP TSG SA WG3 Security — S3#23 **S3-020429**
9 - 12 July 2002
Helsinki, Finland

Work Item Description

Title

Support of the Presence Service Security Architecture

1 3GPP Work Area

	Radio Access
X	Core Network
X	Services

2 Linked work items

Multimedia Messaging Service ~~(22.140)~~
IMS Messaging ~~(22.940)~~
Support of the Presence Capability ~~(22.141)~~
Support of the Presence Service Architecture ~~(23.841141)~~
IMS Group Management ~~(22.250)~~
Access Security for IP-based services ~~(33.203)~~
Network Domain Security ~~(33.210)~~

3 Justification

The presence service results in presence information of a user and information on a user's devices, services and services components being managed by the wireless network. The type of services may include:

- Chat, instant messaging, email and multimedia messaging
- Advanced push services
- Enhanced existing services e.g. voice call converted to text e.g. MMS message
- Presence access list and access control rule

A group list of watchers is maintained in presence service. They are the group that are allowed by the presentity to access the presence information.

The user shall be able in a secure way define access rules to control the access to his/her presence information e.g. status or location. The access rules describes how a watcher may access the presence information. A watcher may have no access, restricted access or full access to the presence information. A watcher may fetch presence information on a regular basis by polling the system or the watcher may subscribe on presence information e.g. be receiving a notification when a change in information has occurred.

There are ~~three~~four possible configurations ~~When~~ regard to the presence Server and the Watcher application ~~resides~~ location~~in an IMS network~~ ~~network there are three possible configurations~~. These configurations and its implications on the security architecture shall be investigated. The configurations are:

1. Presences server and Watcher application located in IMS

2. Presence server located in the IMS and Watcher application located in the external Internet, if the Watcher Application supports the standard Pw interface specified in TS 23.141
3. Presence server located in the external Internet and the Watcher application located in the IMS, if the Presence Server supports the standard Pw interface specified in TS 23.141

The scope of this work item may include other non-IMS based configurations such as WAP based presence suppliers or OSA based watchers.

4 Objective

The objectives of this work item:

- To specify a secure procedure for accessing to and using presence information.
- To define and specify the Stage 2 security ~~requirements~~ architecture ~~such~~ so that the presence information can be accessed by a watcher for different configurations in a secure manner.
- To define and specify the Stage 2 security architecture so that the presence information can be managed by presentity in a secure manner.
- To specify what security related parameters need to be visible and configurable for the user.

5 Service Aspects

~~*Presence service shall support the distribution and availability of presence information to the intended watchers.*~~ *To be linked with S1's feature WID.*

6 MMI-Aspects

To be linked with S1's feature WID.~~*Services exploiting the presence capability, will enable monitoring status information of other users, and enable setting the visibility of users. It shall be specified what security related parameters need to be visible and configurable for the user.*~~

7 Charging Aspects

~~-~~Security aspects related to charging might need to be specified.

8 Security Aspects

Any presence solution must provide a secure procedure to gain access to, and use, presence information. The presence information shall be provided in a secure way such that the receiver can trust the received information. ~~*Also security aspects related to charging might need to be specified.*~~

9 Impacts

Affects:	USIM?	ME	AN	CN	Others
Yes	X	X		X	
No					
Don't know	~~X~~		X		X

10 Expected Output and Time scale (to be updated at each plenary)

The results of this Work Item shall be provided in a Technical Standard or CRs to existing Technical Standards.

The following Work Plan is proposed.

Meeting	Date	Activity
S3#24	July 9-12, 2002	Approval of this WID. ~~Presentation by SA2 to SA3 of system architecture concepts and principles.~~ Analysis of trust model, threats and security requirements. Draft TR.~~Feasibility study and discussion of security principles and requirements.~~??
S3#25	October 8-11, 2002	Definition and agreement on security architecture~~, and CRs~~. Progress the TR.
S3#26	November 19-22, 2002	The required CRs approved.

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.203		Access Security for IP-based services	TSG-SA#18~~5~~	
33.210		Network Domain Security	TSG-SA#~~15~~18	
22.127		Open Service Access (OSA)	TSG-SA#18	

11 Work item raporteurs

Krister Boman, Ericsson~~??????~~
Email: krister.boman@erv.ericsson.se

12 Work item leadership

TSG SA3

13 Supporting Companies

~~Motorola, Siemens, Lucent Technologies, BT, France Télécom, Orange, Ericsson, Nokia, Nortel Networks, NN~~Nokia, Ericsson, Lucent, Nortel Networks, Orange France, Siemens, Hotsip

14 Classification of the WI (if known)

	Feature (go to 14a)
	Building Block (go to 14b)
X	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

(list of Work Items identified as building blocks)

14b The WI is a Building Block: parent Feature

(one Work Item identified as a feature)

14c The WI is a Work Task: parent Building Block
The parent Building Block is “Support of Presence Capability” identified as PRESNC.

3GPP TSG SA WG3 Security — S3#23 **S3-020430**
9 - 12 July 2002
Helsinki, Finland

Work Item Description

Title 3GPP Generic User Profile Security

1 3GPP Work Area

	Radio Access
X	Core Network
X	Services
X	Terminals

2 Linked work items

VHE,
OSA,
Subscription Management,
UE Management,
MExE,
IMS,
MMS,
Presence,
Location Based Services,
Push,
Network Domain Security,
Access Security for IP-based services

3 Justification

3GPP SA WG2 is developing specifications for Generic User Profile in 3GPP. New security requirements have to be developed to support this new functionality, therefore a new 3GPP SA WG3 WI is needed.

4 Objective

The objective of this WI is to evaluate and develop the "Generic User Profile" security requirements, documented in 3G TS 22.240, and to generate the necessary CR's to S3 and S2 specifications.

The scope of this work item includes:

- Authentication and authorisation mechanisms for access to user profile data.

- Integrity protection and confidentiality mechanisms for the transfer of user profile data between core network elements,
- Authentication, Integrity protection and confidentiality mechanisms for transfer of user profile data between the UE and the core network.
- Authentication, Integrity protection and confidentiality mechanisms for transfer of user profile data between third party providers and the core network

5 Service Aspects

Services are customised and personalised by the 3GPP Generic User Profile.

6 MMI-Aspects

The user is able to activate, deactivate, and customise a user profile.

7 Charging Aspects

It shall be possible to support charging for the management and use of user profiles, and for access to user profiles (e.g. alteration of call forwarding).

8 Security Aspects

The work item is a security item. Access to the 3GPP Generic User Profile data shall be performed in a secure and authenticated manner, and the integrity of user profile information shall be assured.

9 Impacts

Affects :	USIM	ME	AN	CN	Others
Yes	X	X		X	X
No			X		
Don't know					

10 Expected Output and Time scale (to be updated at each plenary)

The results of this Work Item shall be provided in a Technical Standard or CRs to existing Technical Standards.

The following Work Plan is proposed.

Meeting	Date	Activity
S3#24	July 9-12, 2002	Approval of this WID. Discussion of security principles and requirements.
S3#25	October 8-11, 2002	Discussion of security principles and requirements and potential solutions. Definition and agreement on security architecture. Agreement of security

		solutions and discuss draft CRs
S3#26	November 19-22, 2002	The required CRs approved

New specifications

Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications

Spec No.	CR	Subject	Approved at plenary#	Comments
33.203		Access Security for IP-based services	TSG-SA#18	
33.210		Network Domain Security	TSG-SA#18	
33.102		Security Architecture	TSG-SA#18	

11 Work item rapporteur

Brad Owen Lucent Technologies
Contact: bvowen@lucent.com
Trigonos
Windmill Business Park
Swindon
Wiltshire SN1 4DW
UK
Tel: +44 1793736245

12 Work item leadership

TSG SA WG3

13 Supporting Companies

Siemens, Ericsson, Motorola, Orange, Nokia, Lucent Technologies

14 Classification of the WI

	Feature (go to 14a)
X	Building Block (go to 14b)
	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

14b The WI is a Building Block: The 3GPP Generic User Profile

14c The WI is a Work Task: parent Building Block

3GPP TSG-SA3 (Security) **S3-020432**
Meeting #24, Helsinki, Finland, 9-12 July 2002

Source: **Vodafone**

Title: **Draft Work Item Description:**
Release 6 User Equipment Management: Security aspects
WI type: Work task

Document for: **Discussion**

Agenda Item: **UEM**

This work item description is based on the draft SA5 UEM Building Block work item description.

Work Item Description

Title: User Equipment Management (UEM): Security aspects

User Equipment Management (UEM) is a capability which will allow the Operator, Service Provider and/or User Equipment Manufacturer/User Equipment Supplier to remotely manage User Equipment.

1 3GPP Work Area

	Radio Access
	Core Network
X	Services
X	Terminals

2 Linked work items

- UEM Building Block (SA5)
- GUP security (SA3)

3 Justification

The UEM feature allows UEs to be remotely managed. The Release 5 UEM feasibility study (TR 32.802) identified a number of security considerations which should be addressed in the standards. This work task is intended to address those security considerations and any others that are identified in the course of the work.

4 Objective

Three key UEM capabilities are identified in TR 32.802 (in priority order with highest priority first):

1) UE Configuration Query capability that allows UE configuration information to be remotely requested and retrieved;

Against this capability TR 32.802 identified the following security considerations:

> "It is essential that the requesting party is authenticated. There should be a valid relationship between the requesting party and the UE owner, for example explicit permission granted to perform the UE Configuration Query.
>
> The UE Configuration Query capability does not change the configuration of the UE.
>
> Integrity protection of the messages on both the downlink and the uplink are required."

2) UE Reconfiguration capability that builds upon the UE Configuration Query capability in that it allows configuration changes to be made to the UE remotely;

Against this capability TR 32.802 identified the following security considerations:

> "The requesting party should be authenticated. There should be a valid relationship between the requesting party and the UE owner, for example explicit permission granted to perform the UE Configuration Query.
>
> Security is even more important for this capability than the UE Configuration Query capability as the UE is being modified. The approach to security could include signing and/or encryption. Integrity protection of the messages on both the downlink and the uplink are required."

3) Remote UE Diagnostics capability to run diagnostic applications on the user equipment to aid fault resolution.

Against this capability TR 32.802 identified the following security considerations:

> "It is essential that the requesting party is authenticated. There should be a valid relationship between the requesting party and the UE owner, for example explicit permission granted to perform the UE Diagnostics Capability. It is essential that UEM is properly authorised, that the UE is satisfactorily protected, that IPR of the UE manufacturers' is protected, that downloads are virus free etc. The downloaded software would need to be encrypted by the UE manufacturer and decrypted on the UE. It should be authenticated that the UE manufacturer has certified the downloaded software. The integrity of the software should be ensured and Integrity protection of the messages on both the downlink and the uplink are required."

At a minimum UEM capability (1) shall be standardised in Release 6.

SA3 will work with the lead groups (SA5 and T2) to ensure that the UEM building block is completed effectively.

It will be investigated whether the security solutions developed for the Generic User Profile may be re-used for UEM.

5 Service Aspects

Not relevant.

6 MMI-Aspects

Some security mechanisms may have impact on the MMI. For example, it may be required to obtain permission from the user before performing UEM interactions. SA3 will work with SA5 and T2 to ensure the UEM MMI aspects are adequately addressed.

7 Charging Aspects

Not relevant.

8 Security Aspects

Security is crucial to UEM and SA3 will ensure the UEM security aspects are adequately addressed.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes	X	X			X
No			X		
Don't know				X	

10 Expected Output and Time scale (to be updated at each plenary)

New specifications						
Spec No.	Title	Prime resp. WG	2ndary resp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments
32.xxx	UEM Requirements and Architecture (Stages 1 & 2)	SA5	T2	TSG#20 (06/03)	TSG#21 (09/03)	
2x.xxx	UEM Protocol Specification	T2		TSG#20 (06/03)	TSG#21 (09/03)	

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments

11 Work item raporteurs

Peter Howard (Vodafone Group) [peter.howard@vodafone.com]

12 Work item leadership

SA3

13 Supporting Companies

(at least 4 companies)
Vodafone Group, Motorola, Hutchison 3G, Siemens.

14 Classification of the WI (if known)

	Feature (go to 14a)
	Building Block (go to 14b)
X	Work Task (go to 14c)

14c The WI is a **Work Task**: parent **Building Block**

Release 6 UEM Building Block (SA5)

3GPP TSG SA WG3 Security — S3#24 S3-020433

9 - 12 July 2002, Helsinki, Finland

Work Item Description

Title

Security Aspects of Multimedia Broadcast/Multicast Service (MBMS)

1 3GPP Work Area

X	Radio Access
X	Core Network
X	Services

2 Linked work items

Multimedia Broadcast Multicast Service – SA
Enhancement of Broadcast and Introduction of Multicast Capabilities – RAN
Support of the Multimedia Broadcast Multicast Service in CN protocols – CN

3 Justification

The Multimedia Broadcast/Multicast Service has some clear security requirements. If these are not met then the service will not satisfy the requirements set by SA1. It is the role of SA3 to ensure that the security requirements are met.

4 Objective

The objective of this work item is to satisfy the security requirements given in TS 22.146 and provide suitable input to SA2 to assist in defining the MBMS architecture.

A crucial requirement of MBMS is to be able to deliver content simultaneously to several users using network resources in an efficient manner. For the Multicast part of the service, users out side the target group should not be able to understand the transmitted data. In order to achieve this requirement, it is necessary to be able to authenticate subscribers and deliver the content in a secured manner.

The lawful Interception aspects of the MBMS will also be considered.

5 Service Aspects

MBMS should allow users to select one of a number of broadcast/multicast information sources, and to share with other users the network resources used to deliver that information.

Service level aspects are agreed in TS 22.146.

Architectural aspects are covered in TR 23.846.

6 MMI-Aspects

None identified

7 Charging Aspects

The ability to charge for access to, and use of, MBMS services shall be supported..

8 Security Aspects

This is a security work item.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes		X		X	
No					
Don’t know	X		X		

10 Expected Output and Time scale (to be updated at each plenary)

The results of this Work Item shall be provided in a Technical Standard or CRs to existing Technical Standards.

The following Work Plan is proposed.

Meeting	Date	Activity
S3#24	July 9-12, 2002	Approval of this WID. Discussion of trust model, threats and security requirements.
S3#25	October 8-11, 2002	Definition and agreement on security architecture for inclusion in the TS
S3#26	November 19-22, 2002	Refinement of the architecture and addition of the security mechanisms
S3#27	February 25-28, 2003	Finish the work of TS

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments
TS 33.xxx	Security of Multimedia Broadcast/Multicast Service	SA WG3		SA#18 (12/02)	SA#19 (03/03)	

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments

11 Work item raporteurs

Adrian Escott, Hutchison 3G UK
Contact : adrian.escott@hutchison3g.com
Star House
20 Grenfell Road
Maidenhead
SL6 1EH
UK
Telephone : +44 7866 600924

12 Work item leadership

TSG SA WG3

13 Supporting Companies

Hutchison 3G UK, Lucent, Alcatel, Vodafone, Ericsson

14 Classification of the WI (if known)

	Feature (go to 14a)
X	Building Block (go to 14b)
	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

(list of Work Items identified as building blocks)

14b The WI is a Building Block: parent Feature

MBMS, 2544

14c The WI is a Work Task: parent Building Block

(one Work Item identified as a building block)

TSG-SA WG 3 (Security) meeting #24 **S3-020451**
Helsinki, Finland, 9-12th July 2002 **Agenda Item:7.9**

Title: **WLAN Interworking Security WID**

Source: **SA WG3**

Work Item Description

Title

WLAN Interworking Security WID

1 3GPP Work Area

X	Radio Access
X	Core Network
X	Services
X	Terminals

2 Linked work items

Access Security for IP based Services
Subscription Management
UE Management
User equipment functionality split
Network Domain Security (if secure distribution of authentication between roaming partners is necessary)
Lawful Interception
WLAN inter-working WID in SA1 and SA2

3 Justification

There is an increasing demand for wireless 'local area' access in very different scenarios. Wireless access to Internet is provided to public users by the use of currently existing WLAN technology such as IEEE 802.11b. In companies wireless access is provided to portable computer users by use of the same technology. For residential use wireless access is also increasing. 3rd generation technologies and systems will provide bearers for similar packet switched services, with greater mobility and wider area coverage albeit with reduced data rate.

WLAN technology can complement 3GPP based networks in deployment environments with high user density and demand for higher data rates. However, in order to provide flexible use of both technologies in these environments and to provide mobility of services between the two technologies it is sensible that some degree of interworking exists between the two technologies/systems.

The current study within SA1, described in the "3GPP system – WLAN Interworking" WID, covers requirements aspects of WLAN-3GPP System Interworking [S1-020638]. In addition SA2 have a complimentary WID, which is identifying and analysing potential Interworking architectures [S2-020908]. It is therefore considered to be necessary for SA3 to develop Security Architecture suitable for implementation to enhance these work items.

4 Objective

In co-ordination with SA1 and SA2, SA3 is to produce a Technical Specification for WLAN Interworking. This document will be developed based on the following deliverables:

1. A review of the security of existing and relevant technologies i.e. IEEE, 3GPP and IETF, including RAN technologies and network technologies

2. An elaboration of a Trust model and inter-working scenarios

3. An analysis of potential threats

4. Recommendations of appropriate access control mechanisms including Authentication, Authorisation, and key management including symmetric as well as asymmetric technologies

5. Recommendations of appropriate mechanisms for the confidentiality and integrity protection for different hops and layers i.e. first hop (e.g. link layer) and network hop (e.g. PIC&IPSec etc)

6. A definition of the security requirements, to include any requirements for Lawful Interception

A preference will be given to solutions that are bearer independent.

These deliverables will then: -

- ❑ Ensure that any changes to the 3GPP Specifications, resulting from this work are implemented within 3GPP via the standard 3GPP CR process.

5 Service aspects

Security architecture will meet the service requirements defined by SA1

6 MMI aspects

MMI aspects will need to address the configuration and visibility within the terminal and the network of the security status from the perspective of both the end user and the service provider.

7 Charging Aspects

None Identified

8 Security Aspects

This is a Security Item

9 Impacts

Affects:	USIM	TE	MT	UE	AN WLAN	AN RAN	CN	Others
Yes	X	X	X	X	X	X	X	
No								
Don't know								

10 Expected Output and Time scale (to be updated at each plenary)

Deliverables				
No.	Title	Prime rsp. WG	Completion Date	Comments
1	3GPP & IEEE WLAN Interworking Security Review	SA3	SA3#25 8-11th October 2002	A Review of the security of existing 3GPP and IEEE WLAN security from a theoretical and practical perspective. http://www.ieee802.org/11/ http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm http://www.cs.umd.edu/~waa/1x.pdf http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html http://slashdot.org/articles/01/02/15/1745204.shtml
2	3GPP & IEEE WLAN Interworking Security Risk Analysis	SA3	SA3#25 8-11th October 2002	Determination of the security risks associated with various deployment environments and interworking scenarios. (SA2 Technical Report will be presented for info at SA #17 9th – 12th September)
3	Wireless Local Area Network (WLAN) Interworking Security Technical Specification		SA3#27 Feb 2003	

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments
TS xx.xxx	Wireless Local Area Network (WLAN) Interworking Security	SA3	SA1 SA2	SA#19 17th – 20th March 2003	SA#20 9th – 12th June 2003	TS To include Trust Model as an informative annex

Affected existing 3GPP specifications				
TS	21.133		3G security; Security threats and requirements	
TS	33.106		Lawful interception requirements	
TS	33.107		3G security; Lawful interception architecture and functions	
TS	33.108		3G security; Handover interface for Lawful Interception	
TS	33.200		Network Domain Security - MAP	
TS	33.203		3G security; Access security for IP-based services	
TS	33.210		3G security; Network Domain Security (NDS); IP network layer security	

Existing IEEE specifications	
IEEE 802.11, 1999 Edition	ISO/IEC 8802-11: 1999) IEEE Standards for Information Technology -- Telecommunications and Information Exchange between Systems -- Local and Metropolitan Area Network -- Specific Requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
IEEE 802.11a-1999	(8802-11:1999/Amd 1:2000(E)), IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Amendment 1: High-speed Physical Layer in the 5 GHz band
IEEE 802.11b-1999	Supplement to 802.11-1999,Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band
IEEE 802.11d-2001,	Amendment to IEEE 802.11-1999, (ISO/IEC 8802-11) Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Operation in Additional Regulatory Domains
IEEE 802.11i	Draft Standard 802.11i, D2.1 (March 2002): Specification for Enhanced Security.

Affected existing specifications ETSI BRAN

ETSI TS101 761-2 V1.3.1	Broadband Radio Access Networks (BRAN) HIPERLAN Type 2 Data Link Control (DLC) layer; Part 2: Radio Link Control (RLC) sublayer.

11 Work item rapporteurs

Luis Lopez-Soria, Ericsson	luis.lopez-soria@ece.ericsson.se
Colin Blanchard, BT Group	colin.blanchard@bt.com

12 Work item leadership

SA3

13 Supporting Companies

Alcatel, BT Group, Ericsson, Gemplus, Lucent, Motorola, Nokia, Nortel, Orange, Siemens Sonera, Telenor, Telia, Vodafone,

14 Classification of the WI (if known)

	Feature (go to 14a)
X	Building Block (go to 14b)
	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

14b The WI is a Building Block:
Parent Feature “Wireless LAN Interworking”.
Leader: SA1

14c The WI is a Work Task: parent Building Block