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 ~~(23.841~~141~~)~~
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.