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)