TSG-SA WG3 (Security) meeting #1 **_TSGS-WG3#1(99)006_**

Docklands, London, 2 - 4 February 1999

Record of Strategic decisions taken by SMG10 (WPC) with regard to UMTS security specification

Introduction

This document contains a list of all the “strategic” decision taken by SMG10 WPC and SMG10 plenary in their development of UMTS security specifications, and the rationale behind these decisions. It has been produced so that these decisions may be collected in one place instead of being spread across many meeting reports. It is hoped that this will allow other bodies to see our reasoning, and also to avoid SMG10 unnecessarily re-visiting issues on which conclusions have been reached.

A “strategic” decision is one which has significant impact on the future development of the security specifications. A decision to specify application layer authentication and integrity for inter-node signalling for instance, would be a strategic decision.

The “date decision taken” column will also include the dates of the ratification of the decision by SMG10 plenary and SMG plenary (the ratification in the latter case will probably take the form of approving a specification in which the decision is present in some way).

References to supporting documents will be given where appropriate. WPC meeting reports going back to Worcester, February, 1998 have been analysed.

Decisions and Rationale

Decision	**Rationale**	**Date decision taken and body responsible**
1. A USIM must be present in a UMTS ME when a UMTS service is being accessed from the ME via a UMTS service provider. This requirement applies whether the service is free or charged, and originating at the ME or terminating.	For chargeable services, the USIM ensures that the identity of the user can be authenticated, and charges billed accordingly. Reliable security services are also impossible without the USIM. For free services, the user identity must also be identified to prevent abuse. In both cases, authenticated user identity is required for legal interception purposes.	WPC, Newbury, 15-16 June, 1998.
2. Incontestable charging is not required for bearer services in UMTS Phase 1	A clear service requirement for this was not apparent. As such, the significant tasks that would be involved in	WPC, Bonn, 21-22 September, 1998.

	developing and implementing incontestable charging for bearer services could not be justified.	
3. Pan-network support for session key establishment for end to end (e2e) security services will not be part of UMTS Phase 1 (though e2e security services are still a long term goal UMTS goal).	It was felt that this was too ambitious a goal for the Phase 1 timescales. In particular, it was believed that the specification of standardised key escrow/recovery for lawful interception purposes would be particularly problematic within the Phase 1 timescales.	WPC, Bonn, 21-22 September, 1998.
4. Ciphering of user data shall terminate at the RNC at least.	The absence of ciphering on the BTS-BSC link in GSM is a significant weakness, as the link is often a microwave link. The equivalent link in UMTS, the node B - RNC link must therefore be ciphered. Continuing the ciphering on the MS - Node B link on to the RNC is more efficient than adopting separate ciphering for the Node B - RNC link.	WPC, Bonn, 21-22 September, 1998.
5. UMTS Phase 1 shall **not** support mutual explicit entity authentication of **serving network**.	It was agreed that there was not a requirement to explicitly authenticate the identity of the serving network for UMTS Phase 1. It was sufficient to trust the HE to only send security related information on its subscribers to legitimate serving networks. HOWEVER, future phases of UMTS may involve a large number of serving networks, and reliance on HE trust of SN’s may become unwieldy or unsatisfactory. Therefore the possibility of requiring explicit entity authentication of the SN is not excluded for future phases of UMTS is not excluded.	SMG10 #4/98, Paris, 17-20 November, 1998.
6. UMTS shall support verification of the authorisation to give services to the user of the serving network by the HE. (This amounts to proof by the SN of possession of a secret related to the user that could only have been provided by the HE)	This can prevent a number of false BTS attacks (specifically non-covert eavesdropping, capture of B-number, set up of spoof call to user, answering of MO user call). Response in verification of serving network must be dependant on user identity or non-covert eavesdropping is possible.	SMG10 #4/98, Paris, 17-20 November, 1998.

7. UMTS Phase 1 shall not support the use of public key techniques for service related authentication.	The gains from the use of public key techniques were not sufficient to justify the extra complexity of public key over secret key techniques. However, the possibility of using public key techniques in future phases of UMTS is not excluded.	SMG10 #4/98, Paris, 17-20 November, 1998.
8. UMTS shall support a framework for service related authentication that gives limited flexibility in the mechanism used for service related authentication.	This will allow future proofing of UMTS - new authentication mechanisms can be introduced if required.	SMG10 #4/98, Paris, 17-20 November, 1998.
9. UMTS shall **not** support verification by the HE that the SN has authenticated the user.	Such verification would require some form of non-repudiation – for example, that as part of service related authentication, the user signs a string that the SN can return to the HE as proof that the user was authenticated. There is not a clear service requirement for this for UMTS Phase 1 (just as there is not a clear service requirement for Incontestable charging, see decision 2).	SMG10 #4/98, Paris, 17-20 November, 1998.
10. UMTS shall not support a two layer (SN and HE) temporary identity scheme.	Such a scheme would not provide extra protection against active attacks as it is presumed a facility for HE's to request the IMSI would still be required. This request could be spoofed by a false BTS. The two layer scheme gives limited extra protection against passive attack but these is not presumed to be the real threat – active attack is.	SMG10 WPC, Herentahls, 15-16 December, 1998.