3GPP1 TSG (Common meeting) **Tdoc TSG#1(98)-012**
Sophia Antipolis 7-8/12/98

Doc For	TSG SA	TSG CN	TSG RAN	TSG T
Decision				
Discussion	X			
Information		X	X	X

Source: **Chairman ETSI/SMG1**0

Title: **Proposals for Treatment of *Security* in UMTS**

Agenda:

Purpose: **Discussion**

Progress

Work on security for UMTS has been underway for some time in ETSI SMG 10., and ETSI SMG has already formally approved (for internal use) the following specifications and reports, which are available on the ETSI Server:

UMTS 33.20 (was 09.01): Security principles for UMTS (version 3.1.0)
UMTS 33.21 UMTS Security requirements (version 1.x.y)
UMTS 33.22 UMTS Security features (version 0.x.y)
UMTS 33.23 UMTS Security mechanisms (version 0.x.y)

From an ETSI perspective the requirements for security in UMTS have now been established, and work has started on specifying the various elements of a security architecture that will satisfy the requirement.

The current principle for inclusion of security features in phase 1 of UMTS may be summarised as follows:

- Adopt all features from GSM that have proved to be needed and workable
- Provide new features that address security weaknesses in GSM which are known to cause concern
- Introduce at least one new, desirable and technically significant security feature into UMTS

Proposals

The security work for UMTS in SMG10 has been undertaken by an ad-hoc working party in conjunction with the SMG 10 plenary.

To continue the work in 3GPP, **it is proposed that a Security Working Group (a 3GPP TSG-SA WP Security) be set up within the System Aspects TSG**

It is likely that many of the present delegates of SMG 10 would wish to contribute to the new group. Work on the security of GSM will continue, as new services and features are introduced, as new threats are unearthed, and as advances in cryptanalysis and the technology needed to breach security are made. There will therefore be considerable synergy between the activities of the two groups, with the same fundamental issues being considered by both. It is therefore to be expected that many delegates will wish to attend both groups. For these reasons it may be desirable to hold the two meetings (SMG 10 and TSG-SA WG Security) together at the same place. In principle one meeting may follow the other, although some of the very system independent security problems may be addressed jointly. Such an approach would minimise delay and disruption, while broadening the scope to include all interested members of 3GPP (who would all be invited to attend the SMG 10 if desired). It is therefore **proposed that SMG 10 and 3GPP TSG-SA WP Security** meetings be jointly held

Attached is a proposal for **terms of reference of a 3GPP TSG-SA WP Security,** which was prepared during the last meeting of SMG 10. As a rough guide, the work already completed by SMG 10 covers 1, 3, 4, 5 and 7, and work is well underway on 6 and 8. **This could be a starting point for the work on UMTS security in 3GPP**

Decisions Needed

TSG-SA is invited to consider the three proposals made above, which may be summarised as follows:

1. Establish a security working group within SA – 3GPP TSG-SA WP Security.
2. Encourage SGG 10 and the newly formed TSG-SA WP Security to hold their meetings together.
3. Consider the terms of reference for the TSG-SA WP Security proposed by SMG 10, and use the work on UMTS already completed or underway in SMG as a starting for its work on security.

DISCUSSION TSG SA, Source Michael Walker , Chairman SMG10

SMG10, meeting #4/98 Tdoc SMG10 98P324
Issy-les-Moulineaux, 17 to 20 November 1998

Suggested Terms of Reference
for
3GPP - System Aspects TSG - Security WG

To build on the work already undertaken for UMTS by ETSI SMG 10 and [*other standards bodies to be added if appropriate*] in order to

1. Determine the objectives and priorities for UMTS security taking into account the needs and aspirations of users, operators, regulators and manufacturers.
2. Accommodate, as far as is practicable, any regional variations in security objectives and priorities for 3GPP partners.
3. Ensure that a threat analysis for UMTS is conducted.
4. Detail the security requirements for UMTS - this to include, but not necessarily be limited to, security requirements for services, billing and accounting, operations and maintenance, and fraud control.
5. Detail the security requirements for the physical elements of UMTS - this to include, but not necessarily be limited to, security requirements for the radio access network, the core network and its interfaces to non-UMTS networks, terminals, UIM and interfaces between UMTS systems.
6. Define a security architecture for UMTS which will satisfy the security requirement and align with the UMTS system architecture.
7. Produce a time and milestones plan for the introduction of the various elements of the security architecture which is in line with the security priorities and the phasing of UMTS.
8. Produce specifications for all the elements in the security architecture - the controls, protocols and functions.
9. Produce specifications for the operations and management of the security elements.
10. Produce requirements specifications for any cryptographic algorithms needed for the security elements.
11. Ensure the availability of any cryptographic algorithms which need to be part of the common specifications.
12. Define how the specifications for the security elements are to be integrated into the radio access, core network, terminal, UIM, O&M and other relevant specifications produced by 3GPP, and to assist with that integration.
13. Detail the requirements for lawful interception in UMTS, and produce all specifications needed to meet those requirements.
14. Produce guidelines on the use of the UMTS security features, including any requirements for operator specific algorithms.
15. Produce guidelines on the limitations of UMTS security, and of the implications of not activating the security features that are provided.
16. Detail requirements that are related to the processing of personal data and privacy, and ensure that UMTS specifications meet them.