**3GPP TSG SA WG3 (Security)** Meeting Report No. 1
London Docklands: 2-4 February 1999

**Source:** **Secretary, TSG SA WG3 (Security)**

**Title:** **Report of TSG SA WG3 meeting #1 (2-4 Feb 99, London, UK)**

**Document for:** **Information**

**Agenda Item:** **9.3**

## 3GPP TSG-S WG Security
## Meeting Number 1
## International Hotel, Docklands, London

## 2-4 February 1999
Start 1030 and finish 1710 on 2 February 1999.
Start 0930 and finish 1700 on 3 February 1999.
Start 0930 and finish 1240 on 4 February 1999.

## 1 Welcome and Introductions
Mike Walker introduced the domestic arrangements. Mike Walker of Vodafone will be the Convenor, Charles Brookson of the Department of Trade and Industry the Secretary of the meeting.

The delegates introduced themselves. The list of participants is in document 019.

## 2 Objectives of the Meeting
Mike Walker gave a presentation of what he saw were the objectives of the meeting:

- Establish terms of reference
- Agree principles for 3G security (Documents to be complete by end this year).
- Specifications- decide what documents we intend to produce
- Set a work program- what will be produced, by when and by whom
- Agree working methods – meetings, project support form 3GPP etc
- Identify relationships – with other 3GPP WGs, with SMG10, with SAGE, ETSI, ARIB etc
- Election of Chairperson, etc. – identify positions, review election process.

2.1 Timetable

| | | |
|---|---|---|
| Tuesday am | Terms of reference | 1-5 |
| pm | Principles | 6-7 |
| Wednesday am | Documentation | 8.1 |
| pm | Work programme and method of working | 8.2-8.4, start 9 |
| Thursday am | Relationships | 9-12 |

2.2 Target output
The target outputs from this meeting are:

- Terms of Reference- detailed TOR proposal to TSG-SA
- Deliverables- list of specifications & other documents we will produce with scopes
- Work programme- timetable, milestones, meeting schedules, work with and from others, support

**Agreed:** There were no comments on the above, this was taken as agreed as a way forward for the Group.

## 3 Approval of the Agenda

**Agreed:** The Agenda was approved.

## 4 Assignment of documents

Documents 001 to 012 presented and assigned to agenda items (see Table below). There were no further documents presented.

## 5 Terms of reference

**Agreed:** There were no objections to using Document 009 as the basis of the terms of reference. It was agreed that 008 should be taken into account.

5.1 Agreed Changes to 009

For the opening Paragraph:
Delete 'SMG 10'.
Change 'UMTS' to 'second and third generation systems' (Per Christoffersson).

Working through the sections of 009:

1) Agreed.
2) Change 'regional' to 'regional/ regulatory' (Nigel Barnes)
3) Agreed.
4) Change 'services, billing' to services, user access to services, billing'.
5) Change 'between UMTS systems' to 'between UMTS networks' (Tim Wright). Change 'UIM' to 'User Identification Module (UIM)'.
6) Change 'security requirement' to 'security requirements'.
7) Agreed, although it needs to be changed in position to between (13) and (14) below.
8) Remove '-the controls, protocols and functions'.
9) Agreed.
10) Agreed.
11) Agreed.
12) Agreed.
13) 'This work shall be performed in conjunction with the regional standards bodies'. In particular with ETSI TC Security should be included in the Requirements Document as the European body to reflect Document 008 and 013 in item 8.1 below.
14) Agreed
15) Agreed.
16) Change to 'Accommodate, so far as is practicable, regional regulatory requirements that are related to processing of personal data and privacy.' Move this to after section (2)

We need to include the words features and mechanisms in the document as we are writing these output documents. (14) and (15) change 'feature' to 'elements'.

Add a final sentence: 'Liaison may be established with the following committees:
SMG10, TC Security, SAGE, 3GPP, ARIB Security Group, and other bodies as required.'

**Agreed:** This will become document 017.The revised document was circulated on 3/2 and approved as the new terms of reference with the following changes:

Items 7 and 14 interchanged
Last paragraph changed '3GPP' to '3GPP working groups'.

## 6 Review of work of Partner Organisations and Principles for 3G Security

6.1 Document 012: Principles for 3G Security
Document principles suggested by Mike Walker in 012 are:

- Build on 2G security: adopt those features from GSM and other 2G systems that have proved to be needed and robust.
- Correct problems with 2G security - 3G must address real and perceived weaknesses in 2G.
- New features – at least one 3G specific security feature.

Gert Roelofsen suggested that the item three above become: New features – provide security for features in 3G that are not in 2G but require securing.

**Agreed:** These principles were accepted with the modification above.

6.2 Elaboration of the Document 012 Principles
Mike Walker presented his thoughts and suggestions:

6.2.1 Principle 1 in 6.1 above:
1) Subscriber authentication – but the algorithm has been a problem.
2) Air – interface encryption – key length is now too short and support for multiple algorithms has caused problems.
3) Subscriber Identity Confidentiality – but a better mechanism is probably needed.
4) SIM – used as a security module manageable by operator independent of terminal.
5) SIM application toolkit security features – providing a secure application layer channel between SIM and network server.
6) Transparency – but visibility is also needed.
7) Trust – should not assume trust between operators.

**Agreed:** 1, 2, 3, 4, 5 {but change' network server' to 'network operator or entity'}, 6, 7 is deleted.
Add statement that 'Trust - should be minimised between operators' to (7).

6.2.2 Principle 2 in 6.1 above:
1) False base station attack
2) Clear transmission of cipher keys and authentication values – triples are transmitted in clear across signalling networks
3) Encryption terminated too soon – user traffic in clear on microwave links.
4) Authentication tied to encryption – authentication relies upon encryption being on, and not all recognise this
5) IMEI – this is an unsecured identity, which has not been treated as such.
6) Fraud and LI – should be considered at design phase (FIGS etc now address this).

**Agreed:** 1, 2, 3, 4, 5, and 6.
(2) Should include 'within and between' networks.
Should look at location services for emergency calls, this may be added to the services group requirements for 3GPP.
No data integrity for non-speech services should be included in the above.
Inflexibility – key lengths and even algorithms should be easily changed.

The new features were discussed in Section 8 below.

## 7 Discussion and agreement on baseline documents

Each of the documents submitted was discussed to identify the base line inputs to 3GPP.

7.1 Doc. 002

This document was agreed by the application group of ARIB IMT-2000 study committee and describes the security design principle and the algorithms.

**Error! Bookmark not defined.**Vol1_08.zip

Phase 1 has been completed; Phase 2 is just being started. The algorithms will be ready by April this year; service will start by the year 2000 (or maybe 2001). The intention is to have one confidentiality algorithm for use in Japan, one for the rest of the world.

**Agreed:** This is a major input paper for principles and requirements.

7.2 Doc. 003 Security Requirements

Presented by Tim Wright.

**Action Point 1:** Theo Metzger, Reg TP Germany to check document 003 to comment by the next meeting if the risk analysis he requests in 008 and 013 is necessary and sufficient as he requested in his input documents.

**Agreed:** This is a major input paper for principles and requirements.

7.3 Doc. 004 Security Features

Presented by Bart Vinck. Status is due for submission to next SMG Plenary.

Has a data integrity mechanism to stop the false base station attack by protecting the signalling channels.

**Agreed:** This is a major input paper for a proposed features document.

7.4 Doc. 005 Security Requirements

Presented by Tim Wright. This document is still in the formative stage.

Has a key lifetime, where they key can only be used a few times. Ciphering will be terminated at the RNC- it could be further into the network. GSM method of TMSI is being used, for key establishment using sequence numbers to ensure triplets cannot be reused. Signalling security is also being introduced, and also security between applications.

**Agreed:** This is a major input paper for architecture and mechanisms.

7.5 Doc. 006

**Agreed:** This is an input paper for architecture and mechanisms, and should be a working methods document in agenda item 9.

7.6 Doc. 10 Tetra 3 change of authentication method

**Agreed:** This is an input paper for architecture and mechanisms, which should be attached to Doc. 005.

7.7 Doc. 11

Document from ARIB.

**Agreed:** This is an input paper for features.

## 8 Construction of a work program

8.1 Type and scope of deliverables

Documents 014, 016, 003, 004, 005, 006,010 discussed as contributions.

Editors should reference these above used in their documents.

8.1.1 Security Objectives and Principles
There will be a top-level document called Security Objectives and Principles including text from 016 and 003.

1. Objectives will go in as three elements to the document, using section 4 (003 Document, 33.21)
2. Requirements will include 2G, 2G+ and new features.

New features suggested were:

- More players- new players (e.g. content providers, service providers), more operators (so more roaming).
- Preferred means of communication – 3G will promote wireless as preferred means.
- Prepaid, do not tie security to subscription method
- Customer access to profiles- customers will set up and modify profiles etc e.g. Over Internet
- Active attacks – security must be robust against attackers impersonating network elements

8.1.2 Security Requirements (to include threat analysis)
Adaptation of ETSI UMTS 33.21 & ARIB ' Requirements … system' version 0.8.

Section 5 of 33.22 to be included to explain the threat analysis. The structure of the document is to be the context, threat identification, requirements, mapping and weighting of threats, and analysis of threats.

8.1.3 Security features
Starting point ETSI UMTS 33.22 (Security features) and document 016.

Authentication derived cipher key, confidentiality, IMEI, user PIN and SIM Lock.
Annex B should become part of the main body of features. There should be a mapping between the requirements and the features.

New features to be included: Network authentication, ciphering indicator, new proposal for identity confidentiality (a single method should be proposed, using a group key to encrypt the IMSI). Should include support for the SIM application toolkit and location services.

8.1.4 Security Architecture and Mechanisms
Starting point ETSI UMTS 33.23 (Security Mechanisms and Architecture) Start point is document 010.

**Agreed:** That the Security features document should become the first part of the Security Architecture and Mechanisms document.

8.1.5 Security Implementation requirements
Requirements on SIM, infrastructure, terminal, etc possibly separate parts. Suggested that it could be an annex at some later stage of a previous document such as architecture.

8.1.6 Cryptographic algorithm requirements
One part on each algorithm is required. Document 016 refers. The draft ciphering algorithm from UMTS needs to be tabled.

8.1.7 Cryptographic Algorithm Specifications
This will only cover common algorithms; they are likely to be designed by a third party

If there is a common algorithm (such as the air interface) then there should be a number of possible methods:

Creation:

1) Algorithm already available (such as a public domain) off the shelf or a modification of an existing algorithm.
2) Invite submissions.
3) Ask someone to design it by commission.

Evaluation:

1) By committee or group experts.
2) By open publications with invitation to respond.
3) Review existing evaluations.

Distribution:

1) Distribution to those who need it under licence.
2) Open publication (give it away).

There should be an option to support several algorithms.

8.1.8 Lawful Interception requirements

To be written using TC Security, SMG 10 and ILETS as a background document.

8.1.9 Lawful Interception architecture and functions

8.1.10 A guide to the 3G security features

Guidelines on the use and limitations, and on the impact on personal data protection etc. To complement to the 'Objectives…' No reference to security assessment and approval record should be within the document.

8.2 Work items

See above.

8.3 Rapporteurs, Editors

**TIMESCALES & DELIVERABLES FOR 3GPP SECURITY**

| **Document** | **Meeting Dates** | **Editor** | **Doc No.** | **Due by** | **Status** |
|---|---|---|---|---|---|
| Objectives and Principles | By Email | Tim Wright | 28 | 1st Draft by 12/2/99. 1st release for TSG one week afterwards. Complete by 1/3/99 | Scope agreed as 021 subject to changes to references. |
| Threats and Requirements | By Email | Per Christoffersson | 29 | 1st list of scope and contents by 12/2/99. 1st draft by end of February. 1st release end March 1999 | Changes to 33.21 for UMTS proposed.<br><br>Scope agreed as 026. 3G Threats and Requirements. |

| | | | | | |
|---|---|---|---|---|---|
| Architecture | 23/02/99 Stockholm | Bart Vinck & Stefan Pütz | 30 | 1st list of scope and contents by 12/2/99.<br>1st draft by end of February.<br>Complete end March 1999 | To be combined with Security Architecture as the first chapter.<br>Adding SIM secure messaging, and that all the security features form the architecture, with examples.<br><br>Scope agreed as 023. |
| Integration Requirements | | Colin Blanchard | 31 | 1st list of scope and contents in Document 020.<br>1st draft by end of March.<br>1st release end of May | List of scope and contents ready Document 020.<br>Updated by document 025.<br>Change to '3G Security, Integration Guidelines'. |
| Cryptographic Algorithm Requirements | | Takeshi Chickawaza | 32 | 1st list of scope and contents end of February.<br>1st draft by end of March.<br>1st release end of May | Gert Roelofsen to provide ETSI documents.<br><br>List of scope and contents given in 024.Modification required supporting encryption, user authentication and use. Some of algorithms may need to be standard, some proprietary. |
| Cryptographic Algorithm Specifications | | Gert Roelofsen responsible for work item. | 34<br><br>Working Doc 37 | 1st list of scope and contents by 12/2/99.<br>1st release end of May | Study of possibilities for acquiring algorithms:<br>For internal circulation to the working group. |
| Lawful Interception requirements | | Berthold Wilhelm | 35 | 1st list of scope and contents end of February.<br>1st draft by end of March.<br>1st release end of May | Should reference documents that exist. Charles Brookson to provide GSM Association document. |
| Lawful | | Berthold | 36 | Scope by | |

| | | | | | |
|---|---|---|---|---|---|
| interception architecture and functions | | Wilhelm (Provisional) | | June 1999 | |
| Guide to the 3G security | | Charles Brookson | 33 | 1st list of scope and contents end of February. 1st draft by end of March. 1st release by September. | |

**Agreed:** Mike Walker to provide the 3GPP document template.
**Agreed**: All editors to include references to documents that they have drawn upon.

Note: All documents to be finished by end 1999.

**Agreed:** It was agreed that the removable SIM would be mandatory for the system. This was not just technical reasons, but also fraud considerations to prevent easy access to sensitive data on terminal equipment. A document is to be drafted by Mike walker for the TSG meeting at the start of March outlining the reasons for the security module or SIM.

**Action Point 2:** That there should be a reference list made by Mike Walker of the documents used and referenced; this 'Dictionary' should indicate if 3GPP documents replace them. Mike Walker should raise this at the TSG.
**Action Point 4:** All editors to note and meet the time scale and documents to be produced in the table.
**Action Point 5:** Mike Walker to write a paper explaining the reasons why the group agreed that the SIM was mandatory for 3GPP security and fraud prevention. Paper to be produced by next

3GPP.8.4 Time scales
See above.

## 9 Working methods and schedule of meetings
See 12 below.

## 10 Process of election of Chairman and Vice Chairman
Candidates need to put forward an application with a CV and a letter of support from their employer. The letters should be the Convenor or Chairman of TSG. Applications are preferred two weeks before, although last minute is possible. Proxies (up to 5) must be in with the paper. There is a registration process for each individual member, contact Ian Doig. Maurice Pope is to elaborate by Email, and that everyone at this meeting should be registered as participants.

The Security Group will have a Chairman and two Vice Chairman. Support is required for the meeting. Elections to be held on Thursday of SMG10 meeting.

## 11 Review of draft report of meeting
This draft report was tabled and sent by Email, comments by 12/02/99.

## 12 Dates and Venues for future meetings

1) A meeting in the last week of February in Schipol Airport for editors and drafting groups.

2) Proposed 3GPP TSG SA WG3 and SMG10 meeting, Stockholm 23-26 March:

| Time | Tuesday | Wednesday | Thursday | Friday |
|---|---|---|---|---|
| Morning | Opening Plenary<br>SMG10 | WPA<br>WPB<br>3GPP | WPA<br>WPB<br>3GPP | Closing 3GPP |
| Afternoon | WPA<br>WPB<br>Start 3GPP | WPA<br>WPB<br>3GPP | Closing SMG10<br>3GPP | |

3) Other meetings scheduled:

| | | |
|---|---|---|
| April | 27/28 | Bonn |
| June | 17/18 | UK |
| August | 3/6 | with SMG10 |
| October | 26/7 | The Hague |
| November | 16/19 | with SMG10 |
| December | 7/8 | Helsinki or Lapland |

## Thanks

The meeting thanked Vodafone; who kindly sponsored the meeting within London Docklands, providing the facilities and Doreen for helping to make the meeting run smoothly.

## ACTION POINT LIST Meeting Number 1.

**Action Point 1/1:** Theo Metzger, Reg TP Germany to check document 003 to comment by the next meeting if the risk analysis is necessary and sufficient as he requested in his input documents.

**Action Point 2/1:** That there should be a reference list made by Mike Walker of the documents used and referenced; this 'Dictionary' should indicate if 3GPP documents replace them. Mike Walker should raise this at the TSG.

.

**Action Point 3/1 :** Mike walker to reply to 014 Liaison statement. Copy to USIM and radio access group.

**Action Point 4/1:** All editors to note and meet the time scale and documents to be produced in the table.

**Action Point 5/1:** Mike Walker to write a paper explaining the reasons why the group agreed that the SIM was mandatory for 3GPP security and fraud prevention. Paper to be produced by next 3GPP.

## LIASON STATEMENTS

| Doc. Ref. | Liaison Statement Number | Title | Sent to: | Status: Sent Received Dates |
|---|---|---|---|---|
| 014 Action Point 3/1 | 1 | Liaison to TSG SA WP3 Variable length of USIM parameters. | By TSG Term Group 3 (USIM) Nice 25-7 January | Received 4/2/99. 16 parameters of 256 bits or less. A length indicator should be included. Mike Walker to draft reply |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## DOCUMENT LIST

| Document Number | Agenda Item | Description | Discussed | Source |
|---|---|---|---|---|
| 1 | | Draft agenda | Y 2/2 am | Chairman |
| 2 | 6 | Vol. 1 Requirements & Objectives for 3G Mobile Services and System (Version 0.8) | Y 2/2 pm | ARIB |
| 3 | 6,7 | 33.21 UMTS Security Requirements | Y 2/2 pm | SMG10 WPC |
| 4 | 6,7 | 33.22 UMTS Security Features | Y 2/2 am | SMG10 WPC |
| 5 | 7 | 33.23 UMTS Security Mechanisms | Y 2/2 pm | SMG10 WPC |
| 6 | 6,7,9 | Record of Strategic decisions taken by SMG10 (WPC) with regard to UMTS security specification | Y 2/2 pm | SMG10 WPC |
| 7 | 8.4 | SMG10 UMTS time scales | | SMG10 WPC |
| 8 | 5 | Proposed work areas for inclusion in 'Terms of Reference' | Y 2/2 am | Theo Metzger, Reg TP Germany |
| 9 | 5 | Suggested Terms of Reference for 3GPP- Systems Access TSG- Security WG | Y 2/2 am | SMG10 sent to first TSG meeting |
| 10 | 6 | Tetra authentication mechanism version 3 | Y 2/2 am | Lucent as a result of WPC |
| 11 | 6 | TTC Work Items for IMT2000- System Aspect TSG | Y 2/2 am | TTC |
| 12 | 6,9 | Proposals for Treatment of Security in UMTS | Y 2/2 am on part | Chairman SMG10 |
| 13 | 5 | Revised version of suggested term of reference | Y 2/2 am | Theo Metzger, Reg TP Germany |
| 14 | 8.1 | Slides: Principles for 3G Security | Y 3/2 am | Convenor |
| 15 | | Liaison to TSG SA WP3 Variable length of USIM parameters. | Y 4/2 am | TSG Term Group 3 (USIM) Nice 25-7 January |
| 16 | 8.1 | Variable length of Security related parameters. Annex 8 Security Design Parameters | Y 3/2 am | ARIB |
| 17 | 5.1 | Revised Suggested Terms of Reference for 3GPP- Systems Access TSG- Security WG | Y 3/2 am agreed | 3GPP |
| 18 | | Revised version of slides- Specifications | Y | Convenor |
| 19 | | List of Participants to 3GPP meeting No 1. | N/A | |
| 20 | | Security Implementation Requirements: Draft UMTS Security Architecture SMG10 99C05 | Y 4/2 am | Colin Blanchard |
| 21 | | Objectives and Principles of 3GPP security | Y 4/2 am | Tim Wright |
| 22 | | Time scales and Deliverables | Y 4/2 am | 3GPP |

| | | | | |
|---|---|---|---|---|
| 23 | | Security Architecture and Mechanisms | Y 4/2 am | Bart Vinck |
| 24 | | Scope of Cryptographic Algorithm Proposals | Y 4/2 am | Takeshi Chikazawa |
| 25 | | Security Implementation Requirements (Scope only) | Y 4/2 am | Colin Blanchard |
| 26 | | Security Threats and Requirements (Scope only) | Y 4/2 am | Per Christoffersson |
| 27 | | Proposal for improved user identity confidentiality | Y, for info 4/2 am | T Mobile & MMO |
| 28 | | Revised document: Objectives | | |
| 29 | | Revised document: Security threats and requirements | | |
| 30 | | Revised document: Architecture | | |
| 31 | | Revised document: Integration Guidelines | | |
| 32 | | Revised document: Cryptographic Algorithm Requirements | | |
| 33 | | Required document: Guide to 3G Security | | |
| 34 | | Cryptographic Algorithm Specifications | | |
| 35 | | Lawful Interception requirements | | |
| 36 | | Lawful interception architecture and functions | | |
| 37 | | Possibilities for Algorithm Specification | Y | Gert Roelofsen |
| 38 | | | | |
| 39 | | | | |