Technical Specification Group Services and System Aspects
Meeting #2, Fort Lauderdale, 2-4 March 1999

TSGS#2(99)044

Source: **TSG SA WG3 Convenor**

Title: **Report of Meeting Number 1 (Presentation slides)**

Agenda Item: **9.3**

3GPP TSG-SA WG3 (Security)

Report of Meeting Number 1

London, Docklands, UK

2-4 February 1999

Convenor - Professor Michael Walker

vodafone

Meeting Objectives

- Terms of Reference - detailed TOR to be proposed to TSG-SA
- Agreed principles for 3G security
- Deliverables - list of specifications & other documents we will produce with scopes
- Work Programme - timetable, milestones, meeting schedule, support

vodafone

Principles for 3G Security

- Build on 2G security - adopt security features from GSM and other 2G systems that have proved to be needed and robust
- Correct problems with 2G security - 3G must address real & perceived weaknesses in 2G
- New features - where differences in 3G call for security features not needed in 2G

vodafone

GSM Security Features to Retain

- Subscriber authentication - but the algorithm has been a problem
- Air-interface encryption - key length is now too short & support for multiple algorithms has caused problems
- Subscriber identity confidentiality - but a better mechanism is probably needed

vodafone

GSM Security Features to Retain (continued)

- SIM - security module, manageable by operator & independent of terminal
- SIM application toolkit security features - providing a secure application layer channel between SIM & home network server
- Transparency - but visibility is also needed

vodafone

Security Problems to Address

- False base stations possible
- Clear transmission of cipher keys & authentication values - triples are transmitted in clear across within and between networks
- Encryption terminated too soon - user traffic in clear on microwave links

vodafone

Security Problems to Address (continued)

- Authentication tied to encryption - authentication relies upon encryption being on, and not all recognise this
- Data integrity - is not provided
- IMEI - this is an unsecured identity, which has not been treated as such

vodafone

Security Problems to Address (continued 2)

- Fraud & LI - should be considered at design phase (now addressed for GSM)
- Trust - GSM security was designed to minimise trust between operators, but controls to monitor trust are inadequate (e.g. checking use of a triple)
- Flexibility - too little (e.g. key lengths)

vodafone

Context for 3G Security

- More players - new players (e.g. content providers), more operators (so more roaming)
- Preferred means of communication - 3G will promote wireless as preferred access
- Prepaid services - do not tie security to subscription model

vodafone

Context for 3G Security (continued)

- Customer access to profiles - customers will set-up and modify profiles etc. over Internet
- More Data - consideration should be given to security of non-voice services
- ‘Active attacks’ - security must be robust against attackers impersonating network elements

vodafone

3G Security Specifications

- Security Objectives & Principles - 3G context, what we intend to achieve (i.e. better security than on fixed networks) & basis for achieving it (i.e. build on 2G); crisp & easy to read
- Security Threats & Requirements - adaptation of ETSI UMTS 33.21 & ARIB 'Requirements.....System' version 0.8

vodafone

3G Security Specifications (continued)

- Security Architecture - this to define all security features and mechanisms, starting point to be ETSI UMTS 33.23 (Security Mechanisms), & ETSI UMTS 33.22 (Security Features)
- Security Implementation Requirements - requirements on SIM, infrastructure, terminal, etc,

vodafone

3G Security Specifications (continued 2)

- Cryptographic Algorithm Requirements
  - one part for each algorithm needed, standard algorithms & those which may be operator specific
- Cryptographic Algorithm Specifications
  - this will only cover standardised algorithms, they are most likely to be designed by another party, paper considering options being produced

vodafone

3G Security Specifications (continued 3)

- Lawful Interception Requirements
- Lawful Interception Architecture & Functions
- A Guide to the 3G Security Features - guidelines on the use and limitations of security features, impact on personal data protection, etc.

vodafone

Timescales & Deliverables for 3GPP Security

Document	Meeting Dates	Editor	Doc. No.	Due by	Status
Objectives and Principles	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. Scope agreed as 026. 3G Threats and Requirements.

vodafone

Timescales & Deliverables for 3GPP Security (continued 1)

Document	Meeting Dates	Editor	Doc. No.	Due by	Status
Architecture	23/ 02/ 99 Stockholm	Bart Vinck & Stefan Pütz	30	1st list of scope and contents by 12/ 2/ 99. 1st draft by end of February. Complete end March 1999.	To be combined with Security Features as the first chapter. Scope agreed as 023.
Integration Requirements		Colin Blanchard	31	1st list of scope and contents in Document 020.	List of scope and contents ready Document 020. Updated by document 025.
				1st draft by end of March. 1st release end of May.	Change to '3G Security, Integration Guidelines'.

vodafone

Timescales & Deliverables for 3GPP Security (continued 2)

Document	Meeting Dates	Editor	Doc. No.	Due by	Status
Cryptographic Algorithm Requirements		Takeshi Chikawaza	32	1st list of scope and contents end of February. 1st draft by end of March. 1st release end of May.	Gert Roelofsen to provide ETSI documents. List of scope and contents given in 024. Modification required supporting encryption, user authentication and use. Some algorithms may need to be standard, some proprietary.
Cryptographic Algorithm Specifications		Gert Roelofsen responsible for work item.	34 Work-ing Doc 37	1st list of scope and contents by 12/ 2/ 99. 1st release end of May.	Study of possibilities for acquiring algorithms: For internal circulation to the working group.

vodafone

Timescales & Deliverables for 3GPP Security (continued 3)

Document	Meeting Dates	Editor	Doc. No.	Due by	Status
Lawful Interception requirements		Berthold Wilhelm	35	1st list of scope and contents end of February. 1st draft by end of March. 1st release end of May.	Should reference documents that exist. Charles Brookson to provide GSM Association document.
Lawful Interception architecture and functions		Berthold Wilhelm (Provisional)	36	Scope by 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.	

vodafone

Meeting Schedule

March	23-26	Stockholm (with SMG10)
April	27-28	Bonn
June	17-18	London
August	3-6	TBD(with SMG10)
October	26-27	The Hague
November	16-19	TBD(with SMG10)
December	7-8	Helsinki

vodafone