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

TSGS#2(99)043

Source: **SA WG3 (Security)**

Title: **3G Security: Security Principles and Objectives**

Version: **0.0.2**

Date: **24-2-1999**

Intellectual Property Rights

Later by 3GPP

Foreword

Later by 3GPP

Introduction

Later by 3GPP

1. Scope

This document gives the objectives and principles of 3GPP security.

The principles state what is to be provided by 3G security as compared to the security of second generation systems. The principles will also ensure that 3G security can secure the new services and new service environments offered by 3G systems.

The objectives give general, high level requirements for 3GPP security which will be expanded upon in [T & R].

The priorities for the implementation of 3GPP security are also given.

2. References

[T & R] "3G Security: Security Threats and Requirements"

Baseline documents:

ETSI 33.21, V2.0.0, "Security Requirements"

ARIB, Volume 1 "Requirements and Objectives for 3G Mobile Services and System (Ver.0.8)", Annex 8

Tdoc s3-99014, 3GPP TSG SA, WG3 (Security), London, 2-4 February, 1999.

3. Definitions and Abbreviations

3.1 Abbreviations

HE	Home Environment
IMEI	International Mobile Equipment Identifier
LI	Lawful Interception
MExE	Mobile Execution Environment
SAT	SIM Application Toolkit
SN	Serving Network
SIM	Subscriber Identity Module

4. 3G Security Principles

There are three key principles behind 3G security:

I. 3G security will build on the security of second generation systems. Security elements within GSM and other second generation systems that have proved to be **needed** and **robust** shall be adopted for 3G security. These elements are listed in section 4.1

II. 3G security will improve on the security of second generation systems - 3G security will address and correct real and perceived weaknesses in second generation systems. The most important of these are given in section 4.2.

III. 3G security will offer new security features and will secure new services offered by 3G

4.1 Second Generation Security Elements to be retained

3G security shall retain (and in some cases develop) the following security elements of second generation systems.

a) Authentication of subscribers for service access

Problems with inadequate algorithms will be addressed. Conditions regarding the optionality of authentication and its relationship to encryption shall be clarified and tightened.

b) Radio interface encryption.

The strength of the encryption will be greater than that used in second generation systems (the strength is a combination of key length and algorithm design). This is to meet the threat posed by the increased computing power available to those attempting cryptanalysis of the radio interface encryption. Problems caused by multiple algorithms[1] will be dealt with.

c) Subscriber identity confidentiality on the radio interface.

However, a more secure mechanism will be provided.

d) The SIM as

a **removable**, **hardware** security module that is

- manageable by network operators
- independent of the terminal as regards its security functionality

a) SIM application toolkit security features providing a secure application layer channel between the SIM and a home network server

Other application layer channels may also be provided.

b) The operation of security features is independent of the user - i.e. the user does not have to do anything for the security features to be in operation.

However, greater user visibility of the operation of security features will be provided to the user.

c) HE trust in the SN for security functionality is minimised

4.2 Weaknesses in Second Generation security

The following weaknesses in the security of GSM (and other second generation systems) will be corrected in 3G security:

(i) Active attacks using a “false BTS” are possible

(ii) Cipher keys and authentication data are transmitted in clear between and within networks

(iii) Encryption does not extend far enough towards the core network resulting in the cleartext transmission of user and signalling data across microwave links (in GSM, from the BTS to the BSC)

(iv) User authentication using a previously generated cipher key (where user authentication using RAND, SRES and A3/8 is not provided) and the provision of protection against channel hijack rely on the use of encryption, which provides implicit user authentication. However, encryption is not used in some networks, leaving opportunities for fraud.

(v) Data integrity is not provided. Data integrity defeats certain false BTS attacks and, in the absence of encryption, provides protection against channel hijack.

(vi) The IMEI is an unsecured identity and should be treated as such.

(vii) Fraud and LI were not considered in the **design phase** of second generation systems but as afterthoughts to the main design work.

(viii) There is no HE knowledge or control of how an SN uses authentication parameters for HE subscribers roaming in that SN.

[1] The method of negotiating which algorithm to be used is open to attack.

(ix) Second generation systems do not have the flexibility to upgrade and improve security functionality over time.

4.3 New Security Features and the Security of New Service Features

The new service features that will be secured cannot be listed at the time of writing. However, the environment in which these features are likely to be developed can be described. 3G security will secure this environment.

The environment in which new services will be developed can be characterised by (but is not limited to) the following aspects:

- There will be new and different providers of services. For example: content providers, data service providers, HLR only service providers.
- 3G mobile systems will be positioned as the preferred means of communications for users. They will be preferable to fixed line systems.
- There will be a variety of prepaid and pay-as-you-go services which may be the rule rather than the exception. A long-term subscription between the user and a network operator may not be the paradigm. (3G security will provide satisfactory security for such systems and will not be content with insecure systems such as GSM Advice of Charge)
- There will be increased control for the user over their service profile (which they might manage over the Internet) and over the capabilities of their terminal (it will be possible to download new services and functions using systems such as MExE and SAT)
- There will be active attacks on users. (In active attacks, equipment is used to impersonate parts of the network to actively cause lapses in security. In passive attacks, the attacker is outside the system and listens in, hoping security lapses will occur).
- Non-voice services will be as important as, or more important than, voice services
- The terminal will be used as a platform for e-commerce and other applications. Multi-application smartcards where the USIM is one application among many can be used with the terminal. The smartcard and terminal will support environments such as Java to allow this. The terminal may support personal authentication of the user using biometric methods.

5 3G Security Objectives

In addition to the above principles for 3G security, there are the high level objectives given below. These will be expanded upon in [T & R].

a) to ensure that information generated by or relating to a user is adequately protected against misuse or misappropriation;

b) to ensure that the resources and services provided by serving networks and home environments are adequately protected against misuse or misappropriation;

c) to ensure that the security features standardised are compatible with world-wide availability. (There shall be at least one ciphering algorithm that can be exported on a world-wide basis (in accordance with the Wassenaar agreement));

d) to ensure that the security features are adequately standardised to ensure world-wide interoperability and roaming between different serving networks.

e) to ensure that the level of protection afforded to users and providers of services is better than that provided in contemporary fixed and mobile networks (including GSM).

f) to ensure that the implementation of 3GPP security features and mechanisms can be extended and enhanced as required by new threats and services.

6. Priorities

As a priority, 3G security will provide the proven second generation security features described in section 4.1 and correct the weaknesses in second generation systems described in section 4.2.

Security for new services and service environments will then be developed as required.