**TSG-SA Working Group 1 (Services) meeting #3**
**Hampton Court, London, 10th-12th May 1999**

*TSGS1#3(99)249*
**Agenda: 4.11**

**SHIELD FROM MOBILE PHONES**

**SMG1 Tdoc 1-99-139**
**S1-99249**

# FEASIBILITY STUDY

## SHIELD FROM MOBILE PHONES

**TSG-SA Working Group 1 (Services) meeting #3** *TSGS1#3(99)249*
**Hampton Court, London, 10th-12th May 1999** **Agenda: 4.11**

**SHIELD FROM MOBILE PHONES** **SMG1 Tdoc 1-99-139**
**S1-99249**

# ontents

# Introduction

The present study provides requirements to protect in the first case, sensitive areas against transmission of high frequency electromagnetic waves particularly from mobile phones and in other circumstances where the output audible signals from mobile phones can be intolerable. The study goes a bit further to set some requirements where the same mechanism for the two cases can be used for different purpose like assisting mobile phones to be an enabler of remote control technologies.

**TSG-SA Working Group 1 (Services) meeting #3** *TSGS1#3(99)249*
**Hampton Court, London, 10th-12th May 1999** **Agenda: 4.11**

**SHIELD FROM MOBILE PHONES** **SMG1 Tdoc 1-99-139**
**S1-99249**

# 1 Scope

The present document conducts a feasibility study on shielding from mobile phones for GSM Rel'99. This feature presents 3 facets of using a shield in the presence of mobile phone, namely:

1. A Shield has the capability to ensure the security measures as demanded by restricted locations indoor or outdoor, and preserve the safety of the public in due course of any interference in the presence of mobile phone.
2. The second aspect of the Shield is to tolerate mobile phones in public /social locations without being perturbed by various chimes from the MS.
3. The third aspect of the Shield is to interact/communicate with the home appliances/ consumer electronics under the commands of the MS. This type of device is an enabler of remote control technologies, i.e. to allow interoperability with the consumer electronics or to extend wireless networking for mobile devices in and around the home.

   The third aspect of the Shield is not anywhere near protecting one's environment but may be used by Mobile User as an enabler among other intercommunications to remotely trigger and control the alarm surveillance at one's intended location.

   This type of mode operation is expected to be slow in taking off compared to the other two types depending on the varying degrees of practicality and versatility.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

[1] GSM 04.08, Digital cellular telecommunications system (Phase 2+); *Mobile radio interface layer 3 specification* (GSM 04.08 version 6.2.0 Release 1997)

[2] GSM 05.01 Digital cellular telecommunications system (Phase 2+); *Physical layer on the radio path; General description* (GSM 05.01 version 6.1.1 Release 1997)

[3] GSM 05.02 Digital cellular telecommunications system (Phase 2+); *Multiplexing and multiple access on the radio path* (GSM 05.02 version 6.3.0 Release 1997)

[4] GSM 03.41, Digital cellular telecommunications system (Phase 2+); *Technical realization of Short Message Service Cell Broadcast (SMSCB)* (GSM 03.41 version 6.1.0 Release 1997)

[5] Specification of the Bluetooth System **-**Vo.8 January 22nd 1999 –Members Access ONLY

[6] Bluetooth website at www.bluetooth.com.

[7] Homerf website at www.homerf.org

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:
**Bluetooth :** a radio frequency technology enabling users to connect to a wide range of computing and telecommunication devices without cables
Example: can support same devices as InfraRed

**HomeRF SWAP:** is an open platform that enables a broad range of interoperable consumer devices to "talk " to each other without being tethered to the home wiring system.

**IRDA:** is used to provide wireless connectivity technologies for devices that would normally use cables for connectivity. It merely point-to-point. Very short-range and narrow angle.

Example: use by notebook, desktop, printers, phone, pagers, modems, LAN access devices, Medical and industrial equipment, watches etc.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

Not applicable

## 3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

SWAP: Shared Wireless Protocol
HOMERF: a trademark of the Home Radio Frequency Group (HRFWG)
ISM: Industrial -Scientific- Medical

# 4 General Description

Shielding from mobile phone is focused on two components. The first component is referred as a Shield and the second component can be a smart sensor to be integrated within the MS.

The Shield can be a network-oriented system or a standalone device, which can be fixed or portable. The Shield acts as a transmitter, which emits continuous radio signals to safeguard the vicinity of SPECIFIC public locations which are sensitive to the interference of Mobile Station or intolerant to mobile ringing tones. The Shield, for this purpose, has limited intelligent functionalities.

The MS when operated under a network system will be remotely deactivated. The MS when operating under a Shield as a standalone device is a receiver, which bears a smart sensor. When spotting the shield beacon, it reconfigures itself to the demanded settings.

Alternatively, for personal use, a shield is an intelligent, interactive device (portable or fixed) configured to attend to the programmable settings of the Mobile Station (MS). In this circumstance, the MS behaves in its usual mode of operation, but has an intelligent capability to communicate with its shield to remotely control one's home environment.

Each type of shields operates independently from one another and has its own security code of operations.

## 4.1 Classes of Shield

The three types of shields for the requested environments are classified as follows:

- Type A- *Mobile Restricted Vicinity:*

With the continuous growth of Mobile phones, Type A is a demanding feature to ensure safeguard and security measures in public locations like airlines, hospitals, nuclear plant etc from interference in presence of mobile phone.

- Type B - *Public Convenient Vicinity*: A convenient feature to suppress chimes of mobile phones (regarded as a nuisance e.g. in Restaurant, Opera etc.) particularly when socializing.
- Type C - *Personal Convenient Vicinity* :

A practical feature for managing or interact with consumer electronic appliances remotely from or around the home, as well as handling incoming calls according to one's personalized preferences

## 4.2 Mode of Configuration

As a RF technology, the three types of Shields are subjected to worldwide regulator groups, and need to work globally.

The zone and size to be protected are determined by the propagation and penetration characteristics of the Inteference signal from the MS. Usually the propagation of RF waves causes a path attenuation which is proportional to $4\pi/\lambda*d^2$ ( where d is the distance between transmitter and receiver and $\lambda$ is the wavelength used) . Typical home or office environments create even larger wave attenuation typically proportional to $4\pi/\lambda*d^3$ above a distance of about 10 meters.

Type A and B shields (as ***standalone devices***) uses low power short radio wavelength (usually around decimeters or less). The beacon signal is digitally transmitted in one-way mode.

*Type A: Mobile Restricted Vicinity*:

- The shield (as ***a standalone device***) via its wireless short-range radio link unimpeded by light-of-sight restrictions, broadcasts its signal continuously within a region up to 50m.
  This class of Shield (as standalone device) requires high-level of security for operations so that theft or misuse of the shield can be tracked down, and cannot be operated without the proper security code.

  An active MS which approaches such a zone detects the strength of the signal generated by the Shield, shall alert the user before reconfiguring itself by switching itself off. This deactivation of MS is related only to the RF part of the access to the wireless communication medium, but the RF portion for the sensor continues to be activated in the presence of the shield transmitter.
  The MS's RF access shall remain in that status as long as MS is in the protected vicinity, but the normal computing facilities on the MS is still functioning.

  ***Emergency call (incoming or outgoing) is also disable (for the simple reason that in such vicinity, a personal emergency call can disrupt the well being of a whole community).***

  Once the MS has moved away from the interference zone, the MS shall activate itself. The MS sets in mode 2.1 or mode 2.3 as stated below. If the Shield is equipped with a timer indicating that zone is temporarily under a protection mode of high frequency portion of the MS, then after the timer has expired, the MS shall re-activate itself in mode 2.1 or mode 2.3.

  *Note: The factory setting of the mobile terminal is pre-programmed to have RF portion of the sensor activated as the default factory setting, and the user can re-program to its preference settings as long as one is not in the Type A's zone.*

- The Shield ***as a network system*** (rather than a standalone device) may be operated under the same GSM frequency band as the existing GSM networks. The additional functionalities/modifications is to use SYSTEM ***INFORMATION MESSAGES*** mapped into the Base Control Channel (BCCH) or ***REMOTE CONTROL capability via Cell Broadcast Channel (CBCH)*** to a "remote control" page as the broadcast signal.
  Thereby, a mobile station, which has been successfully registered with a BTS for receiving incoming calls, will receive the broadcast signal with a warning alert of a remote switched off. Re-activation is up to the user and will be successful if one is no longer in the protected zone.

*Type B: Public Convenient Vicinity*: The shield has less security access than type A for availability but is also protected by some security mechanism.
MS when detecting the protection signals of Shield B re-configures itself accordingly. In this protected mode, only the chimes of the MS are suppressed, that is the volume of the audible output signals of the mobile terminals is lowered.
The MS configures itself to Mode 2.2 see below.
When user is no longer in the vicinity of the Type B shield, MS shall have its ringing tones set back as programmed.
***At this initial stage, no interaction /diversion of calls or other services from the base station/ GSM networks is foreseen.***
***Emergency call is not affected.***

*Type C: Personal Convenient Vicinity :* This Shield is intended for transmission over 100 meter range, and operates on data rate of 2 Mbps burst. It is up to the user to configure and secure one's system. The Shield is a two-way interactive device abiding to the commands issued by the user via one's mobile terminal, assisting in handling incoming calls/ user's subscribed services, connecting with the computing devices, as well as linking to the home electronic appliances.
**Emergency call is not affected.**
The following programmable settings are conceived:

(i) Personal shield attends to the personal settings as programmed by the user on one's mobile with respect to calls/ supplementary services, and to effect the necessary connections with one’s own computer devices

(ii) Personal Shield operates as personal convenient assistance to the user. Each unit of the home electronic appliances will be equipped with a personal interactive convenient shield responding on a one-by-one basis to user's commands.

(iii) Each of the home appliances will be linked on a one-to-many basis where each unit of the home appliances responds to a master unit. The user terminal, in turn, interacts only with the master unit. The master unit is still a slave to the user terminal.

### 4.2.1 Mode of operation

*Mode 2.1:* Mobile terminal activates itself and restoring any personal settings programmed by the user.

*Mode 2.2:* Ringer is switched off, but a polite alert is activated followed by blinking display for incoming calls. Manual intervention is required to operate MS. Normal operation of MS is still retained

*Mode 2.3:* If the mobile terminal refuses to activate itself and is not within the vicinity of Type A class of Shield, a security code followed by a pin code is requested from the user before unlocking an automatic switch off mode.

# 5 CHARACTERISTICS OF SHIELD

## 5.1 Standalone device

- Portable or fixed
- Low power consumption, wiring to the mains via adapter, or Solar / photovoltaic power for continuous protection
- Operate on a timer basis for discontinuous shielding for Type A and B
- Single chip baseband device
- Radio module operates in ISM band (2.45GHz), for a nominal range up to 50m
- Conform to IEEE 802.11 standard , resistant to RF jamming and robust to interference
- Operate at unique frequency
- Fast Frequency hopping transceiver to avoid interference
- Type A and B one -way radio transmitter - require special security mechanism for operation,
- Type C -
  - flexible configuration
  - Flexible packets ( possibly DMI truncated packets) for supporting wide range of applications
  - May combine elements of DECT and IEE802.11 standards
  - Enabler of remote control and concurrent operations of co-located devices on one-to-one or one-to-many devices

## 5.2 Shield as network system

For Type A class – the Shield shall be dedicated to the sole functionalities of protecting the respected areas. It will broadcast continuously its signal and remotely switch the mobile terminals.

# 6 CHARACTERISTICS OF MS Requirements

## 6.1 SMART SENSOR

- Low-cost single chip to accommodate integration within terminal
- Operate in the unrestricted 2.45 GHz ISM 'free band', which is available globally
- Air interface tailored for low power consumption
- Behave as a receiver for Type A & B Shields. Terminal deactivated for handling calls in Type A vicinity, but still accessible for computing exercise. Within Type B vicinity, only terminal ringer is suppressed
- Interactive for Type C Shield Fast Frequency hopping to avoid interference, and to minimise performance degradation ( mainly within Type C mode)

## 6.2 Mobile Station operating under SHIELD's Network system

MS may need additional software functionalities to detect the broadcast signal, and to configure accordingly to the requested settings, and for re-activation.

# 7 Possible solution envisaged for Type A/ B Shield's system

Depending on the technological approach solutions selected, as a **standalone device** the requirements set forth may not impel additional functionalities or enhancements in the existing mobile networks. The operation of the shield in that case, may not rely on an underlying infrastructure of base stations for broadcasting its signals or to communicate. A shield as network system operating as dedicated GSM base station means modifications in several areas of existing GSM technologies.

The following existing technologies can be possible solutions, namely:
(1) Compatible system as GSM Network to be used a Shield
(2) Infrared links (IrDA) or the extended version **AIR**
(3) Home RF- SWAP ( Shared Wireless Access Protocol) an interface to interoperate with PSTN/ISDN and internet, thus enabling a new class of home cordless services
(4) Bluetooth Concept- A radio interface to enable "ad-hoc" connections between portable devices via wireless short-range without line-of-sight
(5) Other suitable systems

## 7.1 Suitable Candidate (s)

(1) Bluetooth Concept is applicable to the three types of shields with some modifications to the current Spec Version 1.0 standardization ***( not yet public to Members)*** to match the air interface requirements.
(2) Compatible to existing GSM network ( see discussion in the Annex)

## 7.2 Air Interface Requirements

If the BLUETOOTH Concept is the most appropriate solution, then a modified value of the Link Budgets parameters for Terminal and Shield as outlined in the ANNEX need to be ***determined*** .
***A comparison of each wireless option of 2.4GHz ISM band frequency-hopping wireless standards is also outlined in the annex***.

# 8. Security Requirements

General:  The three types of Shields are standalone device, and do not co-exist in the same coverage to form a shield short-range network. It shall be able to operate in the ISM band -2.45GHz.  Each type of Shield will be physically distinguishable from each other.

Initialization:
No mutual authentication with any network is necessary if Bluetooth concept is considered.
If GSM Network is adopted, other validation procedures need to be determined

Registration:

All Shields will bear a registration identity.

Type A will require formal authorization procedures and registration for obtaining installation 's approval to prevent any mishandling and misuse.  Type A will invoke special security mechanism (such as certification Authority, Certification Authenticity and legal validity) including security code together with personal pin code to operate, and to be protected against theft.

Type B Shield's will be allocated mostly to business units which invoke public gatherings /socialising events. It is also protected by a security code and pin code against theft.  It can be activated and deactivated accordingly by the owner.

Type C Shield being mostly for personal/home use, hence the security mechanism shall be configured and invoked according to the user’s personalised preferences.

# Annex :
# Suitable Technologies for Shield Requirements.

## 1. GSM Network option

Using GSM alike system may provide the solution for the shield requirements. This approach will involve modifications to several areas in existing GSM technology -infrastructure, network and radio planning, Services, Mobile Management etc.

## 2. General IrDA characteristics

IrDA transceivers are inexpensive. IrDA has extended its range of standard to include an Area infra Red proposal or **AIR.** The new air proposal extends the range to 8 meters with a data rate of 250 Kbps, and a point-to-point connectivity at a beam angle of 120 rather than 30.

Characteristics of Current IrDA include :

♦ Proven worldwide universal cordless connection.
♦ Installed base of over 50 million units.
♦ Wide range of supported hardware and software platforms.
♦ Designed for point-to-point cable replacement.
♦ Backward compatibility between successive standards.
♦ Narrow angle (30 degree) cone, point-and-shoot style applications. (Non-interference with other electronics and low-level security for stationary devices.)
High data rates; 4 Mbps currently, 16 Mbps under development.

But both IrDA and AIR suffer the following drawbacks:

➢ Limited range (being only one or two meters or even recent eight meters )
➢ Beam sensitiveness to direction, (Line-of-sight is crucial)
➢ Unlikeness for simultaneous communication between more than one units

## 3. Home RF-SWAP (Shared Wireless Access Protocol) option

SWAP enables a broad range of consumer devices to interoperate by establishing an open industry specification for unlicensed RF digital communications for PCs and consumer devices anywhere, in and around the home. Home RF can easily integrate with TCP/IP and interoperates with the PSTN (Public Switched Telephone Network) or ISDN. It offers a range of 50 meters and number of active connections to be around 128 at a time, and about 50 hops per sec

### *HOMERF main parameters are:*

- Frequency hopping network: 50 hops/second
- Frequency range: 2400MHz ISM band
- Transmission power: 100mW
- Data Rate: 1 Mbps using 2FSK modulation, 2 Mbps using 4FSK modulation
- Range: Covers typical home and yard
- Supported stations: Up to 127 devices per network
- Voice connections: Up to 6 full duplex conversations
- Data security: Blowfish encryption algorithm (over 1 trillion codes)
- Data compression: LZRW3-A algorithm
- 48-bit Network ID: simultaneous connections of co-located devices

It is appropriate to handle **Type C Shield** if the mobile user is aiming at controlling one’s home security system, heating/air conditioner or electronic appliances, or interpreting a wireless office at home.
Home RF Swap does not quite fit at this early stage to the Type A and B Shields' requirements as stated above.

# 4. Bluetooth System option

Bluetooth is a proposed Radio Frequency (RF) specification for short-range, point-to-multipoint voice and data transfer. Bluetooth can transmit through solid, non-metal objects. Its nominal link range is from 10 cm to 10 m, but can be extended to 100 m by increasing the transmit power. Bluetooth is a radio interface. It is based on a low-cost, short-range radio link in the 2.45GHz frequency range band. It enables "ad-hoc" connections between small, portable devices via wireless short-range radio links without any need of line-of-sight.
General Bluetooth Characteristics include:

- Operates in the 2.4 GHz Industrial-Scientific-Medical (ISM) bands.
- Uses Frequence Hop (FH) spread spectrum, which divides the frequency band into a number of hop channels. During a connection, radio transceivers hop from one channel to another in a pseudo-random fashion.
- Supports up to 8 devices in a piconet (two or more Bluetooth units sharing a channel).
- Built-in security.
- Non line-of-sight transmission through walls and briefcases.
- Omni-directional.
- Supports both isochronous and asynchronous services; easy integration of TCP/IP for networking.
- Regulated by governments worldwide.
- Enablers of connection to a wide range of computing and telecommunications devices without the need of cables.
- Enable opportunities for rapid, ad hoc connections, and in the future, possibly for automatic, unconscious, connections between devices.
- Bluetooth's power-efficient radio technology can be used in many of the same devices that use IR

## 4.1 AIR INTERFACE Parameters

The following air interface parameters for both the Terminal and the Shield need to be worked out for the best compromise regarding sensitivity, robustness and power consumption etc.

**LINK BUDGETS FOR TERMINAL AND**
**SHIELD ( mainly Type A & B)**

| ***Receiver*** | TERMINAL/<br>Mobile station |
|---|---|
| RX sensitivity | |
| IP 3 | |
| CP 1 dB | |
| Double-sided IF bandwidth | |
| C/I co-channel (0.1% BER) | |
| C/I 1MHz (0.1% BER) | |
| C/I Š 2MHz (0.1% BER) | |
| C/I AWGN (0.1% BER) | |
| In-band image rejection (100 kHz BW) | |
| 30 MHz – 1 GHz | |
| 1 – 12.75 GHz | |
| Max. input level (0.1 % BER) | |
| ***Transmitter*** | **SHIELD** |

TX power:

- Nominal
- Optional range

Modulation index (no ISI)
TX carrier initial offset
TX carrier drift (One slot package)
Adjacent channel power:
± 550kHz
± 1 channel
± 2 channels
± ≥ 3 channels
Out of band spuriousness @ 100 kHz BW:
30 MHz – 1 GHz, operational
30 MHz – 1 GHz, idle
1 – 12.75 GHz, operational
1 – 12.75 GHz, idle
1.8 – 1.9 GHz, any case
5.15 – 5.3 GHz, any case
Power control requirements: optional range
SFDR

***Frequency Sources***
Symbol timing accuracy
Channel-switching time
TX/RX turnaround time

***General***
Antenna diversity
Operating environment when applicable

# 5. System Comparison of 2.4GHz ISM band frequency-hopping wireless standards

| **Name** | **IEEE802.11 FHSS** | **Bluetooth** | **HomeRF** |
|---|---|---|---|
| **Data Rate [Mbps]** | *1.0 / 2.0* | *1.0* | *1.0 / 2.0* |
| **Range [Meters]** | *100* | *10 / 100* | *50* |
| **Min. hop rate [Hz]** | *2.5* | *320* | |
| **Typ. Hop rate [Hz]** | *51* | *1600* | *50* |
| **Modulation method** | *2-FSK / 4-FSK* | *2-FSK* | *2-FSK / 4-FSK* |
| **Modulation index** | *0.32 / 0.16* | *0.32* | *0.32 / 0.16* |
| **Channel switching [µs]** | *224* | *220* | *300* |
| **RX/TX turnaround [µs]** | *224* | *220* | |
| **RX/TX switching [µs]** | *19* | | *25* |
| **Osc. P noise L [dBc/Hz @ 500kHz]** | *-92* | *-89* | |
| **Osc. P noise L [dBc/Hz @ 2MHz]** | *-117* | *-121* | |
| **RX sens [dBm]** | *-80 @ 3% FER* | *-70 @ 0.1 % BER* | *-76 @ 0.1 % BER* |
| **RX IP3 [dBm]** | *-28 @ 3% FER* | *-16 @ 0.1 % BER* | |

| | | | |
|---|---|---|---|
| **RX CP 1dB [dBm]** | | *-26* | |
| **BOM Cost Initial/Volume [US$]** | *150 / 50* | *25 / 5* | *30 / 8* |
| **TX power [dBm]** | *30* | *0 / 20* | *17* |
| **Max # of nodes** | *~10 per net* | *8 + 248 inactive* | *> 128* |

# 6. Other Systems

***Radio frequency systems*** yield a good coverage range per transmitted power. A long range is therefore possible, depending on selected transmit power, receiver sensitivity, wavelength, and anticipated interference. Omnidirectional radiator can be implemented easily, resulting in almost circular or spherical ranges. Radio frequency waves pass through some obstacles and encounter inflection, depending on the selected wavelength, therefore a line of sight between transmitter and receiver is usually not required

As an example, the protection system could be implemented using Bluetooth as the basic standard.

***Optical systems*** typically have a short range per transmitted power. Radiators are usually directional such as in the case of an LED. Some gain in range or transmit power reduction can be achieved by concentration of radiation. Omnidirectional radiators are big and heavy. Scattering can remove the restrictions of directional radiators at the expense of transmit power. Optical systems can be implemented in a cost effective way, particularly the transmitter can be very cheap. System approval can be obtained easily. Radiation does not pass through most of the common obstacles such as walls or furniture, which can be a desired feature. A line of sight path between transmitter and receiver is usually required. Optical systems generate little interference to other devices or services. Few health considerations arise from their use.

As an example, the protection system could be implemented using infrared technology e.g. from home appliance remote controls as the basic standard.

***Acoustic systems*** typically have a short to medium range. The required transmit power per range obtained is rather high. Typical systems have a directional radiator such as a piezoelectric speaker. Acoustic waves are scattered, inflected and reflected by most of the usual objects in home or office environments, therefore a line of sight between transmitter and receiver is usually not required. Radiation does not pass through most of the common obstacles such as walls, windows, and furniture.  System approval can be obtained easily. Acoustic systems generate little interference to other devices or services and only few health considerations arise from their use.

As an example, the protection system could be implemented using ultrasonic technology e.g. from home appliance remote controls as the basic standard.