

RECOMMENDATION ITU-R M.1078

SECURITY PRINCIPLES FOR FUTURE PUBLIC LAND MOBILE
TELECOMMUNICATION SYSTEMS (FPLMTS)

(Question ITU-R 39/8)

(1994)

TABLE OF CONTENTS

	<i>Page</i>
1. Introduction	110
2. Scope	110
3. Structure of the Recommendation	111
4. Related documents	111
5. Definitions	112
6. System overview	112
6.1 System assumptions relevant to security	112
6.2 Operational scenario and logically involved parties (logical parties)	113
7. Considerations	118
8. Recommendations	118
8.1 General objectives for security	118
8.2 System requirements on security	119
8.3 Security provided by FPLMTS	121
8.4 Security management	124
8.5 Security architecture and procedures	124
8.6 Security algorithms	124
Annex 1 – Vocabulary	124
Annex 2 – Threat and risk analysis	126
Annex 3 – Potential security procedures	135

1. Introduction

Future public land mobile telecommunications systems (FPLMTS) are third generation mobile systems (TGMS) which are scheduled to start service around the year 2000 subject to market considerations. They will provide access, by means of one or more radio links, to a wide range of telecommunication services supported by the fixed telecommunication networks (e.g. PSTN/ISDN), and to other services which are specific to mobile users.

A range of mobile terminal types is encompassed, linking to terrestrial or satellite-based networks, and the terminals may be designed for mobile or fixed use.

Key features of FPLMTS are:

- high degree of commonality of design worldwide,
- compatibility of services within FPLMTS and with the fixed networks,
- high quality,
- use of a small pocket-terminal worldwide.

FPLMTS are defined by a set of interdependent ITU Recommendations, of which this one on security principles is a member.

The subject matter of FPLMTS is complex and its representation in the form of Recommendations is evolving. To maintain the pace of progress on the subject it is necessary to produce a sequence of Recommendations on a variety of aspects. The Recommendations strive to avoid apparent conflicts between themselves. Nevertheless, future Recommendations, or revisions, will be used to resolve any discrepancies.

Due to the particular radiating nature of wireless communications, FPLMTS needs to incorporate some security measures to prevent easy reception by more parties than the intended recipient. In addition, the nature of mobile communication of FPLMTS requires security measures to prevent fraudulent access to the services.

2. Scope

The scope of this Recommendation is to provide the principles and framework for the security provided by FPLMTS. The Recommendation covers all aspects of security for FPLMTS, and is intended as a basis for more detailed aspects of FPLMTS security to be integrated in various ITU-R or ITU-T Recommendations including FPLMTS requirements at a later stage.

The Recommendation identifies the security requirements for FPLMTS and defines security features for FPLMTS. An informative Annex to the Recommendation contains a threat and risk analysis including the justification for the various security features defined. The system requirements on security in this Recommendation do not imply any legal responsibilities of involved parties concerning the security of the communication and associated information as this will be in accordance with a country's national law.

Possible security mechanisms, implementation requirements for FPLMTS security mechanisms as procedures between the different parties involved in the FPLMTS operation and security algorithms are, however, not covered in this Recommendation, as these will be covered in the future ITU-R Recommendation on FPLMTS security procedures. The management of security features will be dealt with in the future ITU-R Recommendation on FPLMTS Network Management.

The security provisions recommended for FPLMTS are defined with the objective of ensuring interoperability with roaming across international and national network boundaries. Flexibility is left for implementation within these constraints.

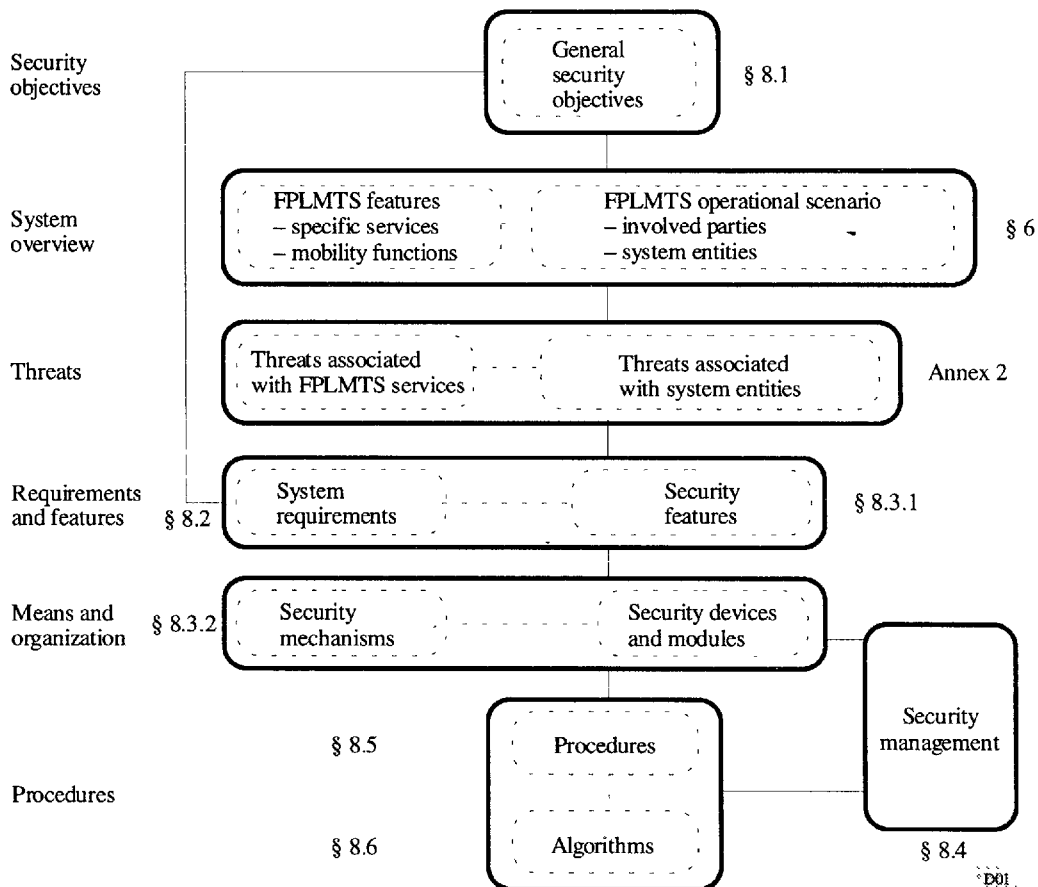
Although there are security requirements and features which are clearly considered to be specific to the radio access, there are those which may not be directly related to the radio access but may still have some relevance to the radio access. They are included in this Recommendation with an indication of "possibly not directly related to the radio interface".

3. Structure of the Recommendation

Figure 1 gives an overview of the methodology and structure of this Recommendation. Section 6 gives a system overview of FPLMTS and identifies the involved parties in the FPLMTS service. Section 8.1 lists the general objectives for security. Section 8.2 gives system requirements on security and § 8.3 identifies the security features provided by FPLMTS, and makes reference to the future Recommendation on FPLMTS security mechanisms.

Section 8.4 is a reference to future Recommendations on FPLMTS network management. Sections 8.5 and 8.6 are reference to the future Recommendation on FPLMTS security procedures and security algorithms, respectively. Finally, Annex 1 lists the vocabulary used in this Recommendation and Annex 2 gives the threat and risk analysis leading up to the security defined for FPLMTS. Annex 3 lists potential security procedures to be considered for the future Recommendation on FPLMTS security procedures.

FIGURE 1
Methodology and recommendation structure



4. Related documents

The following ITU documents contain information on FPLMTS relating to this Recommendation:

- Recommendation ITU-R M.687: Future Public Land Mobile Telecommunication Systems (FPLMTS)
- Recommendation ITU-R M.816: Framework for services supported on Future Public Land Mobile Telecommunication Systems (FPLMTS)

- Recommendation ITU-R M.817: Future Public Land Mobile Telecommunication Systems (FPLMTS) *Network architectures*
- Recommendation ITU-R M.818: Satellite operation within Future Public Land Mobile Telecommunication Systems (FPLMTS)
- Recommendation ITU-R M.819: Future Public Land Mobile Telecommunication Systems (FPLMTS) for developing countries
- Draft ITU-T Recommendation F.115: Operational and service provisions for FPLMTS
- Recommendation ITU-R M.1034: Requirements for the radio interface(s) for Future Public Land Mobile Telecommunication Systems (FPLMTS)
- Recommendation ITU-R M.1035: Framework for radio interface(s) and radio sub-system functionality for Future Public Land Mobile Telecommunication Systems (FPLMTS)
- Recommendation ITU-R M.1036: Spectrum considerations for implementation of Future Public Land Mobile Telecommunication Systems (FPLMTS) in the bands 1 885-2 025 MHz and 2 110-2 200 MHz
- Recommendation ITU-R M.1079: Speech and voiceband data performance requirements for Future Public Land Mobile Telecommunication Systems (FPLMTS)

5. Definitions

A partial list of definitions pertinent to this Recommendation is found in Annex 1.

6. System overview

6.1 System assumptions relevant to security

The following assumptions with possible impact on the FPLMTS security architecture are made:

- a) FPLMTS will be provided in a multi-network operator and multi-service provider environment, public or private, of which some are in direct competition. It can be expected that all parties involved in FPLMTS will have their own security policies;
- b) FPLMTS will be operated across international and national network boundaries with international and national roaming capabilities;
- c) FPLMTS will have an open architecture, based on IN and TMN concepts;
- d) FPLMTS supports UPT;
- e) FPLMTS will provide a variety of services with a range of bit rates. More than one service may be used simultaneously, and the services and/or their bit rates may vary during communication;
- f) FPLMTS will provide a range of terminal types, including integrated terminals as well as terminals with standard interfaces for wired connection to other standard terminals;
- g) FPLMTS users and terminals are logically identified with different unique identities;
- h) a FPLMTS user has a personal service profile, to which he has direct access. This service profile contains personal data of the FPLMTS user, and the FPLMTS user and subscriber have limited ability to modify some of this data. Service profile data include the services subscribed to for the FPLMTS user by the FPLMTS subscriber, various subscription options and a range of service parameters.

The maximum operational scenario of possible involved parties is illustrated in Fig. 2. It should be noted that parties not directly involved in the day-to-day FPLMTS service provision and operation, like regulators, type approval authorities etc. are not included. It should also be noted that Fig. 2 represents the general scenario when a FPLMTS user is called by another user (incoming FPLMTS call), and vice versa (outgoing FPLMTS call). The case of mobile-to-mobile FPLMTS calls is simply a combination of the two, and is for simplicity not included in the figure.

The maximum operational scenario of involved parties in the FPLMTS service use and provision includes the following logical parties:

- the FPLMTS users,
- the FPLMTS mobile terminals,
- the FPLMTS subscribers,
- the home FPLMTS service providers,
- the visited FPLMTS service providers,
- the FPLMTS network operators,
- the FPLMTS terminal manager,
- the mobile FPLMTS transit operators,
- the FPLMTS access providers,
- other network operators,
- other users,
- intruders.

It should be noted that as FPLMTS will provide international roaming with local access to radio resources, the visited FPLMTS service provider may be involved in a call, in addition to the home FPLMTS service provider. Further, as FPLMTS supports UPT, the following parties may additionally be involved:

- the UPT users,
- the UPT subscribers,
- the UPT service providers.

In the following sections, the responsibilities and functions of these FPLMTS parties (security domains) are defined from a security perspective. This does not preclude additional non-security related responsibilities and functions being associated with these parties.

6.2.1 The home FPLMTS service provider role

The home FPLMTS service provider role has responsibility for furnishing services to FPLMTS users, subject to restrictions in service capabilities of the FPLMTS networks that are involved in the service provision, and handling all information related to the subscription associated with a FPLMTS user. A set of user identities logically belongs to the home FPLMTS service provider.

The home FPLMTS service provider role is responsible for mapping FPLMTS numbers on to FPLMTS user identities and/or to FPLMTS mobile terminal identities.

Note 1 – A key item for further study is the implications for fraud of the use of terminal identities and their relationship to user identities.

The association of a FPLMTS number to a FPLMTS user identity is always static, unless there are administrative changes in the FPLMTS subscriptions or FPLMTS numbering plans, while the association of a FPLMTS user identity to a FPLMTS mobile terminal identity may be static or dynamic during normal FPLMTS operation at the choice of the home FPLMTS service provider together with his FPLMTS subscribers. FPLMTS user identities of multiple FPLMTS users may be mapped onto a single FPLMTS mobile terminal identity.

Note 2 – A key issue for further study is whether or not it is useful to allow more than one FPLMTS user to be associated with a FPLMTS mobile terminal identity simultaneously, as it is in any case possible for UPT users. The situation is different for incoming and outgoing FPLMTS calls. For outgoing calls, only one FPLMTS user may be associated at one time, since only one FPLMTS outgoing call could be placed from a FPLMTS mobile terminal at one time. For incoming calls, the situation is different, and more than one FPLMTS user may be considered associated with one FPLMTS mobile terminal identity simultaneously.

The home FPLMTS service provider may use either the FPLMTS user identity or the FPLMTS mobile terminal identity in the communication with the visited FPLMTS service provider in order to reach the FPLMTS user or mobile terminal, respectively.

The home FPLMTS service provider uses the FPLMTS mobile terminal identity in communication with the FPLMTS network operator in order to reach the FPLMTS user. It should be noted that FPLMTS network operators will not necessarily know the FPLMTS user identities explicitly.

The home FPLMTS service provider role carries responsibility for authentication of the FPLMTS users and management of user authentication information. The home FPLMTS service provider may deny the FPLMTS users/subscribers access to the services under certain circumstances.

The home FPLMTS service providers have roaming agreements with a range of visited FPLMTS service providers. There will have to be security mechanisms in FPLMTS such that the home FPLMTS service provider can openly share information with the visited FPLMTS service provider, and vice versa.

Note 3 – Further study is needed on the relationships and relative responsibilities of network operators and service providers with regard to roaming users.

6.2.2 The visited FPLMTS service provider role

The visited FPLMTS service provider has a roaming agreement with the home FPLMTS service provider and is responsible to support the FPLMTS users of the home FPLMTS service provider who roam into the network of a FPLMTS network operator having a direct connection with it.

6.2.3 The FPLMTS network operator role

The FPLMTS network operator is responsible for providing network access to FPLMTS mobile terminals and service capabilities to FPLMTS users roaming into his network, and handles all information related to the communication for all FPLMTS mobile terminals and users in his coverage areas.

The FPLMTS network operator is responsible for:

- location management,
- the allocation of temporary routing numbers.

The FPLMTS network operator handles some FPLMTS user and subscription information when FPLMTS users roam in his network. This information is, however, only restricted to the information required for normal operation and is only indirectly associated with the FPLMTS user identities.

FPLMTS user identities do not logically belong to the FPLMTS network operator role, thus the FPLMTS network operator does not necessarily have any knowledge about FPLMTS numbers or explicit FPLMTS user identities.

The FPLMTS network operator is however responsible for the correct operation and functioning of the FPLMTS mobile terminals accessing his network. Encryption and decryption of FPLMTS radio interface information is also carried out locally by the FPLMTS network operator.

6.2.4 The FPLMTS terminal manager role

The FPLMTS terminal manager is responsible for the FPLMTS mobile terminal identities and is ultimately responsible for the authentication of the FPLMTS mobile terminals and the management of terminal authentication information. The FPLMTS terminal manager may record FPLMTS mobile terminal identities, to facilitate the denial of access to the services under certain circumstances.

The FPLMTS terminal manager may be an independent party or may be embedded in the FPLMTS service provider and/or the FPLMTS network operator.

The decision on the role of the FPLMTS terminal manager needs further study.

Note 1 – The use of the FPLMTS terminal manager and a FPLMTS mobile terminal identity for mobility management and other purposes and its authentication are for further study. It has not been decided yet if other technical realizations should be recommended instead. The benefit and cost of possible solutions shall be assessed before a decision is made.

6.2.5 *Other network operators*

There may be several categories of other network operators:

- intermediate fixed network operators between the home FPLMTS service provider and the FPLMTS network operator (e.g. inter-exchange carriers), or
- intermediate fixed network operators between the originating or destination fixed network operator and the FPLMTS network operator (e.g. inter-exchange carriers), or
- the originating or destination fixed network operator (e.g. local-exchange carriers).

Whatever the category of other network operators, they do not require any call-by-call knowledge of FPLMTS security related information, and do not participate in the call-by-call FPLMTS security procedure. FPLMTS security related information will either:

- never be passed across these operators' networks, or
- be protected when passing across them, or
- be meaningless to them.

6.2.6 *The mobile FPLMTS transit operator role*

There may be two categories of mobile FPLMTS transit operator:

- an operator of a mobile base station (e.g. in buses, trains, ships, etc.), or
- a FPLMTS satellite (space segment) operator.

The mobile FPLMTS transit operators will always relay security related information transparently in both directions. Encrypted information will not be decrypted by the mobile FPLMTS transit operator. The mobile FPLMTS transit operator will not have access to any authentication or encryption keys or algorithms, and is thus to be seen as any third party over the FPLMTS radio interface or a category of other network operators from a security perspective.

Note 1 – A mobile transit operator in this sense is a party which is independent from the FPLMTS network operator (e.g. the mobile transit operator could be a satellite space segment operator and the FPLMTS network operator could be a satellite ground segment operator). It should be noted that these two parties may also be the same. However, in this case, the mobile FPLMTS transit operator is simply another FPLMTS network operator.

6.2.7 *The FPLMTS access provider role*

The FPLMTS access provider is responsible for furnishing FPLMTS radio access to FPLMTS users in a limited coverage area, but does not provide wide-area roaming functionality. In order to provide roaming outside his coverage area, the FPLMTS access provider must rely on a FPLMTS network operator.

Note 1 – A FPLMTS access provider may, for example, be a hotel or a company providing FPLMTS wireless access to its customers/employees. A FPLMTS access provider may, for example, also be a domestic FPLMTS operator (domestic cordless user).

The FPLMTS access provider may have agreements with a FPLMTS network operator or with a fixed network operator, depending on the functionality and roaming that is required. From a security perspective, the FPLMTS access provider carries out all the functions otherwise carried out by the FPLMTS network operator.

Note 2 – In principle, access providers (e.g. domestic cordless users) may have mobile terminals/users without any association with any home FPLMTS service provider or FPLMTS terminal manager. However, in this case, these mobile terminals/users do not have any FPLMTS numbers or FPLMTS user/mobile terminal identities, and are as such not part of the global FPLMTS system. For FPLMTS operation, there is always an associated home FPLMTS service provider and FPLMTS terminal manager.

6.2.8 *The FPLMTS mobile terminal*

The FPLMTS mobile terminals are on the open market and have unique FPLMTS mobile terminal identities. The FPLMTS mobile terminal identity may be assigned by the FPLMTS terminal manager at the time of registration or may be allocated in advance.

The FPLMTS mobile terminals may carry out the actual encryption and decryption (ciphering) of FPLMTS radio interface information.

6.2.9 *The FPLMTS user*

A FPLMTS user is associated with a FPLMTS subscriber.

The FPLMTS user has a unique FPLMTS user identity, which is assigned by the home FPLMTS service provider at subscription time and cannot be changed unless caused by administrative changes to the subscription. The FPLMTS user also has a unique FPLMTS number.

The FPLMTS user may wish to have access to his personal FPLMTS service profile for status information or to modify service parameters. This implies limited real-time interactive access to the service profile data of the home FPLMTS service provider, and FPLMTS user authentication is also needed for this feature. Details of this feature are for further study.

6.2.10 *The user association*

Associating the user with the FPLMTS mobile terminal is accompanied by the capability of the home FPLMTS service provider authenticating the FPLMTS user. The user association needs to be user friendly.

An example of the realization of the user association is the use of the user identity module (UIM) which is logically distributed to the FPLMTS user by the home FPLMTS service provider at the time of subscription. The UIM contains at least the FPLMTS user identity, its authentication key and the data for the user identity module holder verification and may also contain the user authentication algorithm. The UIM may be integrated in the FPLMTS mobile terminal or may be capable of being physically detached from the FPLMTS mobile terminal.

The user association with the FPLMTS mobile terminal could be assisted by the network capability. An example of such a realization uses a voice recognition technique for authenticating the user and determining the user identity. The voice recognition function could be in the FPLMTS network operator or the FPLMTS service provider, while the key information for the user authentication resides in the home FPLMTS service provider.

6.2.11 *The FPLMTS subscriber*

A FPLMTS subscriber is responsible for the charges incurred by his associated FPLMTS users. A FPLMTS subscriber is associated with one or several FPLMTS users. However, this is purely an administrative relationship, and the FPLMTS subscriber is not involved in the normal FPLMTS operation.

The FPLMTS subscriber may have a FPLMTS subscriber identity, and he may wish to have access to the service profiles of his associated FPLMTS users, one by one or all together, to obtain status information or to modify service parameters for his associated FPLMTS users. This implies limited real-time interactive access to the user profile data of the home FPLMTS service provider, and FPLMTS subscriber authentication is needed for this feature. Details of this feature are for further study.

6.2.12 *Other users*

Other users may be of two categories:

- users making calls to FPLMTS users (calling parties), or
- users receiving calls from FPLMTS users (called parties).

Whatever the category of other users, they do not have any knowledge of FPLMTS security related information, and do not participate in the FPLMTS security procedure except in specific cases.

An example of such specific cases may be some interactions between the security services expected by the other user and those offered to the FPLMTS user.

6.2.13 *Intruders*

Intruders are parties that abuse the FPLMTS network or services, either to compromise the confidentiality of the FPLMTS users' information or to defraud the FPLMTS service providers network operators, terminal managers and/or other logical parties.

6.2.14 *The UPT user*

In connection with FPLMTS, the UPT user gains access to UPT services via a FPLMTS radio interface.