RECOMMENDATION ITU-R M.1078

SECURITY PRINCIPLES FOR INTERNATIONAL MOBILE TELECOMMUNICATIONS-2000 (IMT-2000)

(Question ITU-R 39/8)

(1994)

TABLE OF CONTENTS

Page

1. Introduction 2
2. Scope 2
3. Structure of the Recommendation 3
4. Related documents 3
5. Definitions 4
6. System overview 4
   - 6.1 System assumptions relevant to security 4
   - 6.2 Operational scenario and logically involved parties (logical parties) 5
7. Considerations 10
8. Recommendations 10
   - 8.1 General objectives for security 10
   - 8.2 System requirements on security 11
   - 8.3 Security provided by IMT-2000 13
   - 8.4 Security management 16
   - 8.5 Security architecture and procedures 16
   - 8.6 Security algorithms 16

Annex 1 – Vocabulary 16

Annex 2 – Threat and risk analysis 18

Annex 3 – Potential security procedures 27

1. Introduction

International Mobile Telecommunications-2000 (IMT-2000) 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 IMT-2000 are:

– high degree of commonality of design worldwide,

– compatibility of services within IMT-2000 and with the fixed networks,

– high quality,

– use of a small pocket-terminal worldwide.

IMT-2000 are defined by a set of interdependent ITU Recommendations, of which this one on security principles is a member.

The subject matter of IMT-2000 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, IMT-2000 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 IMT-2000 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 IMT-2000. The Recommendation covers all aspects of security for IMT-2000, and is intended as a basis for more detailed aspects of IMT-2000 security to be integrated in various ITU-R or ITU-T Recommendations including IMT-2000 requirements at a later stage.

The Recommendation identifies the security requirements for IMT-2000 and defines security features for IMT-2000. 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 IMT-2000 security mechanisms as procedures between the different parties involved in the IMT-2000 operation and security algorithms are, however, not covered in this Recommendation, as these will be covered in the future ITU-R Recommendation on IMT-2000 security procedures. The management of security features will be dealt with in the future ITU-R Recommendation on IMT-2000 Network Management.

The security provisions recommended for IMT-2000 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”.

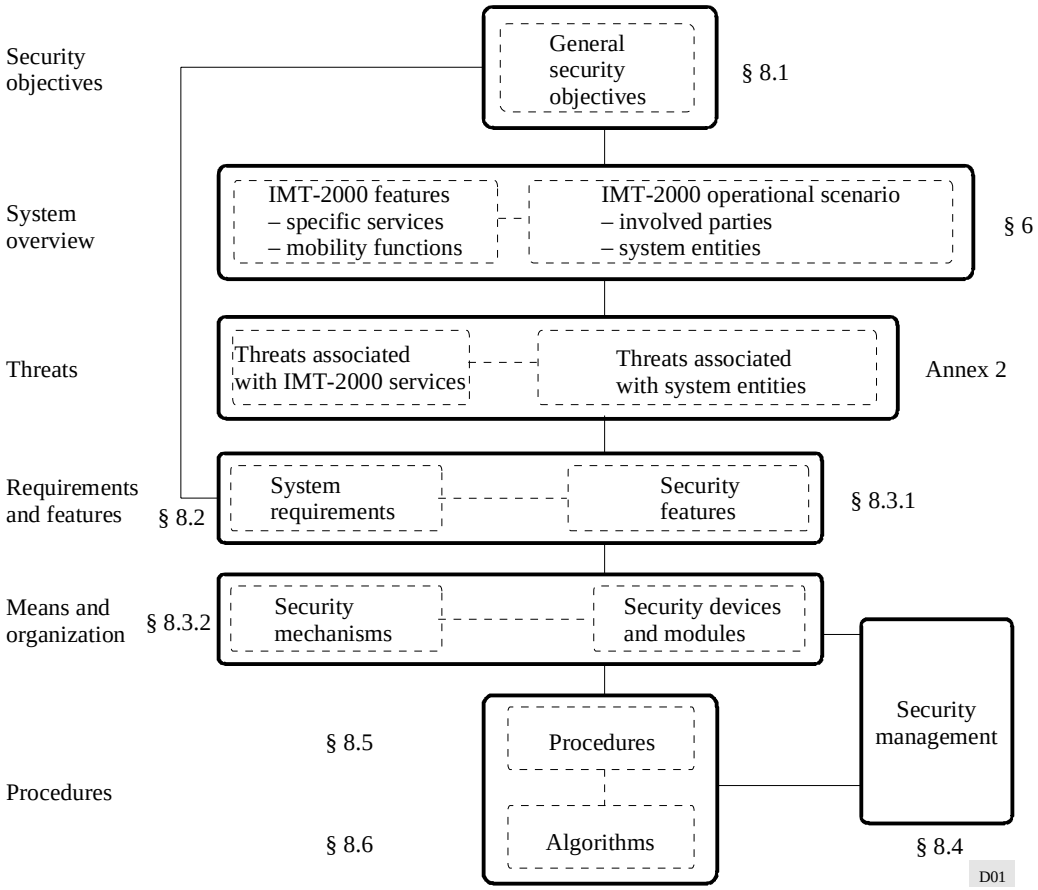
3. Structure of the Recommendation

Figure 1 gives an overview of the methodology and structure of this Recommendation. Section 6 gives a system overview of IMT-2000 and identifies the involved parties in the IMT-2000 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 IMT-2000, and makes reference to the future Recommendation on IMT-2000 security mechanisms.

Section 8.4 is a reference to future Recommendations on IMT-2000 network management. Sections 8.5 and 8.6 are reference to the future Recommendation on IMT-2000 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 IMT-2000. Annex 3 lists potential security procedures to be considered for the future Recommendation on IMT-2000 security procedures.

FIGURE 1

Methodology and recommendation structure



4. Related documents

The following ITU documents contain information on IMT-2000 relating to this Recommendation:

– Recommendation ITU-R M.687: International Mobile Telecommunications-2000 (IMT-2000)

– Recommendation ITU-R M.816: Framework for services supported on International Mobile Telecommunications-2000 (IMT-2000)

– Recommendation ITU-R M.817: International Mobile Telecommunications-2000 (IMT-2000) *Network architectures*

– Recommendation ITU-R M.818: Satellite operation within International Mobile Telecommunications-2000 (IMT-2000)

– Recommendation ITU-R M.819: International Mobile Telecommunications-2000 (IMT-2000) 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 International Mobile Telecommunications-2000 (IMT-2000)

– Recommendation ITU-R M.1035: Framework for radio interface(s) and radio sub-system functionality for International Mobile Telecommunications-2000 (IMT-2000)

– Recommendation ITU-R M.1036: Spectrum considerations for implementation of International Mobile Telecommunications-2000 (IMT-2000) 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 International Mobile Telecommunications-2000 (IMT-2000)

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 IMT-2000 security architecture are made:

a) IMT-2000 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 IMT-2000 will have their own security policies;

b) IMT-2000 will be operated across international and national network boundaries with international and national roaming capabilities;

c) IMT-2000 will have an open architecture, based on IN and TMN concepts;

d) IMT-2000 supports UPT;

e) IMT-2000 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) IMT-2000 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) IMT-2000 users and terminals are logically identified with different unique identities;

h) An IMT-2000 user has a personal service profile, to which he has direct access. This service profile contains personal data of the IMT-2000 user, and the IMT-2000 user and subscriber have limited ability to modify some of this data. Service profile data include the services subscribed to for the IMT-2000 user by the IMT-2000 subscriber, various subscription options and a range of service parameters.

6.2 Operational scenario and logically involved parties (logical parties)

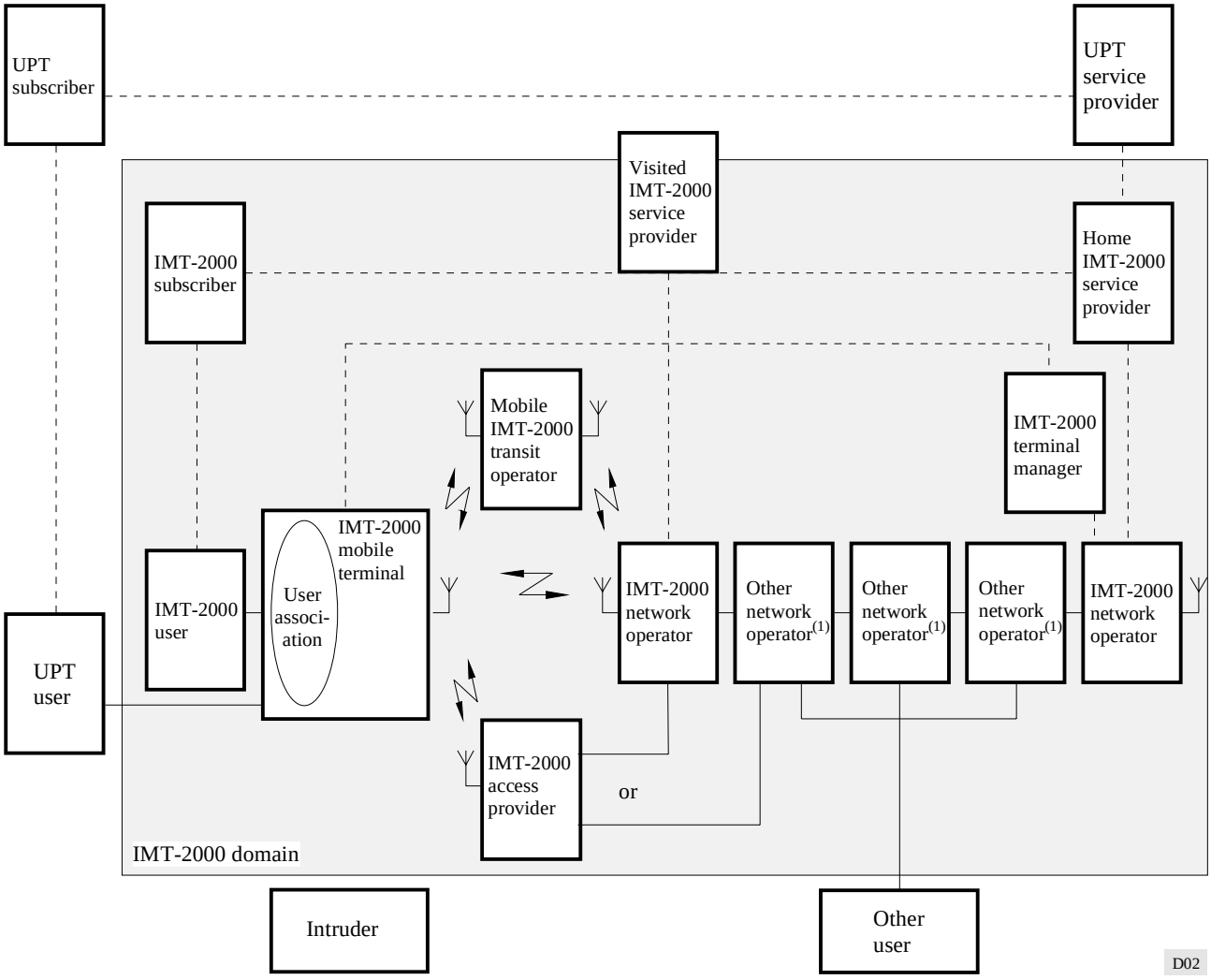
This section defines the operational scenario for IMT-2000 from a security perspective, by identifying all the various logical parties potentially involved in the normal operation of the IMT-2000 service use and provision. This maximum operational scenario is defined concerning the various logical parties involved, thus allowing flexibility and the possibility for different regulatory environments in different countries or regions.

It should be noted that this scenario represents logical parties (roles) involved in the IMT-2000 service use and provision, and does not represent an actual legal entity, person or machine. It is the maximum operational scenario, and some of the parties may not exist in some cases or may be grouped together in one single entity. For example, in a certain environment, the IMT-2000 home or visited service provider and the IMT-2000 network operator could be a single entity. It should further be noted that although the maximum operational scenario is identified in order to define requirements for the overall security of the IMT-2000 service provision and use, its detailed definition may not be part of this Recommendation in all areas, only areas relevant to security.

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 IMT-2000 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 an IMT-2000 user is called by another user (incoming IMT-2000 call), and vice versa (outgoing IMT-2000 call). The case of mobile-to-mobile IMT-2000 calls is simply a combination of the two, and is for simplicity not included in the figure.

FIGURE 2

IMT-2000 operational scenario and logical parties



(1) These operators may or may not be in the IMT-2000 domain.

The maximum operational scenario of involved parties in the IMT-2000 service use and provision includes the following logical parties:

– the IMT-2000 users,

– the IMT-2000 mobile terminals,

– the IMT-2000 subscribers,

– the home IMT-2000 service providers,

– the visited IMT-2000 service providers,

– the IMT-2000 network operators,

– the IMT-2000 terminal manager,

– the mobile IMT-2000 transit operators,

– the IMT-2000 access providers,

– other network operators,

– other users,

– intruders.

It should be noted that as IMT-2000 will provide international roaming with local access to radio resources, the visited IMT-2000 service provider may be involved in a call, in addition to the home IMT-2000 service provider. Further, as IMT-2000 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 IMT-2000 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 IMT-2000 service provider role

The home IMT-2000 service provider role has responsibility for furnishing services to IMT-2000 users, subject to restrictions in service capabilities of the IMT-2000 networks that are involved in the service provision, and handling all information related to the subscription associated with an IMT-2000 user. A set of user identities logically belongs to the home IMT-2000 service provider.

The home IMT-2000 service provider role is responsible for mapping IMT-2000 numbers on to IMT-2000 user identities and/or to IMT-2000 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 an IMT-2000 number to an IMT-2000 user identity is always static, unless there are administrative changes in the IMT-2000 subscriptions or IMT-2000 numbering plans, while the association of an IMT-2000 user identity to an IMT-2000 mobile terminal identity may be static or dynamic during normal IMT-2000 operation at the choice of the home IMT-2000 service provider together with his IMT-2000 subscribers. IMT-2000 user identities of multiple IMT-2000 users may be mapped onto a single IMT-2000 mobile terminal identity.

Note 2 – A key issue for further study is whether or not it is useful to allow more than one IMT-2000 user to be associated with an IMT-2000 mobile terminal identity simultaneously, as it is in any case possible for UPT users. The situation is different for incoming and outgoing IMT-2000 calls. For outgoing calls, only one IMT-2000 user may be associated at one time, since only one IMT-2000 outgoing call could be placed from an IMT-2000 mobile terminal at one time. For incoming calls, the situation is different, and more than one IMT-2000 user may be considered associated with one IMT-2000 mobile terminal identity simultaneously.

The home IMT-2000 service provider may use either the IMT-2000 user identity or the IMT-2000 mobile terminal identity in the communication with the visited IMT-2000 service provider in order to reach the IMT-2000 user or mobile terminal, respectively.

The home IMT-2000 service provider uses the IMT-2000 mobile terminal identity in communication with the IMT-2000 network operator in order to reach the IMT-2000 user. It should be noted that IMT-2000 network operators will not necessarily know the IMT-2000 user identities explicitly.

The home IMT-2000 service provider role carries responsibility for authentication of the IMT-2000 users and management of user authentication information. The home IMT-2000 service provider may deny the IMT-2000 users/subscribers access to the services under certain circumstances.

The home IMT-2000 service providers have roaming agreements with a range of visited IMT-2000 service providers. There will have to be security mechanisms in IMT-2000 such that the home IMT-2000 service provider can openly share information with the visited IMT-2000 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 IMT-2000 service provider role

The visited IMT-2000 service provider has a roaming agreement with the home IMT-2000 service provider and is responsible to support the IMT-2000 users of the home IMT-2000 service provider who roam into the network of an IMT-2000 network operator having a direct connection with it.

6.2.3 The IMT-2000 network operator role

The IMT-2000 network operator is responsible for providing network access to IMT-2000 mobile terminals and service capabilities to IMT-2000 users roaming into his network, and handles all information related to the communication for all IMT-2000 mobile terminals and users in his coverage areas.

The IMT-2000 network operator is responsible for:

– location management,

– the allocation of temporary routing numbers.

The IMT-2000 network operator handles some IMT-2000 user and subscription information when IMT-2000 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 IMT-2000 user identities.

IMT-2000 user identities do not logically belong to the IMT-2000 network operator role, thus the IMT-2000 network operator does not necessarily have any knowledge about IMT-2000 numbers or explicit IMT-2000 user identities.

The IMT-2000 network operator is however responsible for the correct operation and functioning of the IMT-2000 mobile terminals accessing his network. Encryption and decryption of IMT-2000 radio interface information is also carried out locally by the IMT-2000 network operator.

6.2.4 The IMT-2000 terminal manager role

The IMT-2000 terminal manager is responsible for the IMT-2000 mobile terminal identities and is ultimately responsible for the authentication of the IMT-2000 mobile terminals and the management of terminal authentication information. The IMT-2000 terminal manager may record IMT-2000 mobile terminal identities, to facilitate the denial of access to the services under certain circumstances.

The IMT-2000 terminal manager may be an independent party or may be embedded in the IMT-2000 service provider and/or the IMT-2000 network operator.

The decision on the role of the IMT-2000 terminal manager needs further study.

Note 1 – The use of the IMT-2000 terminal manager and the IMT-2000 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 IMT-2000 service provider and the IMT-2000 network operator (e.g. inter-exchange carriers), or

– intermediate fixed network operators between the originating or destination fixed network operator and the IMT-2000 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 IMT-2000 security related information, and do not participate in the call-by-call IMT-2000 security procedure. IMT-2000 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 IMT-2000 transit operator role

There may be two categories of mobile IMT-2000 transit operator:

– an operator of a mobile base station (e.g. in buses, trains, ships, etc.), or

– an IMT-2000 satellite (space segment) operator.

The mobile IMT-2000 transit operators will always relay security related information transparently in both directions. Encrypted information will not be decrypted by the mobile IMT-2000 transit operator. The mobile IMT-2000 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 IMT-2000 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 IMT-2000 network operator (e.g. the mobile transit operator could be a satellite space segment operator and the IMT-2000 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 IMT-2000 transit operator is simply another IMT-2000 network operator.

6.2.7 The IMT-2000 access provider role

The IMT-2000 access provider is responsible for furnishing IMT-2000 radio access to IMT-2000 users in a limited coverage area, but does not provide wide-area roaming functionality. In order to provide roaming outside his coverage area, the IMT-2000 access provider must rely on an IMT-2000 network operator.

Note 1 – An IMT-2000 access provider may, for example, be a hotel or a company providing IMT-2000 wireless access to its customers/employees. An IMT-2000 access provider may, for example, also be a domestic IMT-2000 operator (domestic cordless user).

The IMT-2000 access provider may have agreements with an IMT-2000 network operator or with a fixed network operator, depending on the functionality and roaming that is required. From a security perspective, the IMT-2000 access provider carries out all the functions otherwise carried out by the IMT-2000 network operator.

Note 2 – In principle, access providers (e.g. domestic cordless users) may have mobile terminals/users without any association with any home IMT-2000 service provider or IMT-2000 terminal manager. However, in this case, these mobile terminals/users do not have any IMT-2000 numbers or IMT-2000 user/mobile terminal identities, and are as such not part of the global IMT-2000 system. For IMT-2000 operation, there is always an associated home IMT-2000 service provider and IMT-2000 terminal manager.

6.2.8 The IMT-2000 mobile terminal

The IMT-2000 mobile terminals are on the open market and have unique IMT-2000 mobile terminal identities. The IMT-2000 mobile terminal identity may be assigned by the IMT-2000 terminal manager at the time of registration or may be allocated in advance.

The IMT-2000 mobile terminals may carry out the actual encryption and decryption (ciphering) of IMT-2000 radio interface information.

6.2.9 The IMT-2000 user

An IMT-2000 user is associated with an IMT-2000 subscriber.

The IMT-2000 user has a unique IMT-2000 user identity, which is assigned by the home IMT-2000 service provider at subscription time and cannot be changed unless caused by administrative changes to the subscription. The IMT-2000 user also has a unique IMT-2000 number.

The IMT-2000 user may wish to have access to his personal IMT-2000 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 IMT-2000 service provider, and IMT-2000 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 IMT-2000 mobile terminal is accompanied by the capability of the home IMT-2000 service provider authenticating the IMT-2000 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 IMT-2000 user by the home IMT-2000 service provider at the time of subscription. The UIM contains at least the IMT-2000 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 IMT-2000 mobile terminal or may be capable of being physically detached from the IMT-2000 mobile terminal.

The user association with the IMT-2000 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 IMT-2000 network operator or the IMT-2000 service provider, while the key information for the user authentication resides in the home IMT-2000 service provider.

6.2.11 The IMT-2000 subscriber

An IMT-2000 subscriber is responsible for the charges incurred by his associated IMT-2000 users. An IMT-2000 subscriber is associated with one or several IMT-2000 users. However, this is purely an administrative relationship, and the IMT-2000 subscriber is not involved in the normal IMT-2000 operation.

The IMT-2000 subscriber may have an IMT-2000 subscriber identity, and he may wish to have access to the service profiles of his associated IMT-2000 users, one by one or all together, to obtain status information or to modify service parameters for his associated IMT-2000 users. This implies limited real-time interactive access to the user profile data of the home IMT-2000 service provider, and IMT-2000 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 IMT-2000 users (calling parties), or

– users receiving calls from IMT-2000 users (called parties).

Whatever the category of other users, they do not have any knowledge of IMT-2000 security related information, and do not participate in the IMT-2000 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 IMT-2000 user.

6.2.13 Intruders

Intruders are parties that abuse the IMT-2000 network or services, either to compromise the confidentiality of the IMT-2000 users' information or to defraud the IMT-2000 service providers network operators, terminal managers and/or other logical parties.

6.2.14 The UPT user

In connection with IMT-2000, the UPT user gains access to UPT services via an IMT-2000 radio interface.

The methods for access to the UPT service via an IMT-2000 radio interface are outside the scope of IMT-2000 and are dealt with in Recommendations ITU-T F.850 and ITU-T F.851.

6.2.15 The UPT subscriber

A UPT subscriber is defined in Recommendations ITU-T F.850 and ITU-T F.851. A UPT subscriber does not have any direct connection with IMT-2000.

6.2.16 The UPT service provider

A UPT service provider is defined in Recommendations ITU-T F.850 and ITU-T F.851. In connection with IMT-2000, UPT service providers have agreements with IMT-2000 service providers for provision of UPT services via IMT-2000 networks.

7. Considerations

In developing this Recommendation the following factors were considered:

a) the need for the quality of service of IMT-2000 to be comparable to that of the PSTN/ISDN;

b) the increasing importance of the various types of non-voice telecommunication services;

c) due to the particular radiating nature of wireless communication, it permits easy reception by more parties than the intended recipient;

d) that, concrete steps must as a minimum be taken in IMT-2000 to promote the privacy of communication over the radio interface and to prevent fraudulent service usage;

e) the system overview given in § 6;

f) the relevant ITU-T and ITU-R Recommendations and ongoing studies;

g) that satellite operation within IMT-2000 could facilitate the development of telecommunications services in developing countries;

h) the need for a flexible system structure able to match network investment to the revenue growth, to adapt readily to environmental factors and to respond to new developments without restricting innovation;

j) the need for mobile terminals (including those with satellite capability) to roam between mobile telecommunication networks in different countries;

k) that IMT-2000 will be required to operate in a multitude of environments, each characterized by different propagation characteristics as well as different traffic density and mobility characteristics;

l) that satellite operation within IMT-2000 hold the possibility of significantly enhancing the overall coverage and attractiveness of the services.

8. Recommendations

The ITU Radiocommunication Assembly recommends the following for the security principles for IMT-2000.

8.1 General objectives for security

The following general objectives for security in IMT-2000 apply:

– the security provided to an IMT-2000 user should be comparable to the security provided by the contemporary fixed networks;

– the security provided to an IMT-2000 service provider or network operator should be comparable to the security provided by the contemporary fixed networks;

– the legal, regulatory and commercial aspects of the security provided by IMT-2000 should accommodate worldwide availability;

– the security to be provided by IMT-2000 should be adequately standardized to provide secure worldwide interoperability and roaming between different service providers and/or network operators;

– provision should be made, so that legal interception of a user's communication be possible in accordance with national law;

– IMT-2000 should not utilize security provisions which are inherent features of the radio interface design so that any radio interface design can be adopted without diminishing the security and privacy.

8.2 System requirements on security

System requirements on security are given in this section. They apply to one or more of the parties involved in the IMT-2000 service.

System requirements on security in a general sense may relate to one or more of the following security features:

– confidentiality,

– authentication,

– integrity,

– authorization and access control,

– privacy and anonymity,

– service availability,

– event limitation,

– event reporting.

The system requirements on IMT-2000 security are grouped into the following categories:

– service related requirements,

– access related requirements,

– radio interface related requirements,

– terminal related requirements,

– user association related requirements,

– charging related requirements,

– network operational requirements,

– security management requirements.

8.2.1 Service related requirements

The following service related requirements on security apply to IMT-2000:

– security features provided for the protection of the IMT-2000 users should be user-friendly and easy to use. They should, as far as possible, be transparent to the users, and should require a minimum of user-interactions on a per call basis;

– security features provided for the protection of the IMT-2000 users should not significantly increase call set-up times;

– security features provided for the protection of the IMT-2000 users should work without reduced security during handover and when roaming;

– security features provided by IMT-2000 should work within the various radio environments of IMT-2000, and not be constrained by any one physical layer or access method;

– the privacy of non-IMT-2000 users should not be adversely affected in working with IMT-2000 equipment or services;

– it should be possible under controlled circumstances for information over the IMT-2000 bearer channel to be transmitted in the clear. In the event of encryption failure, identified emergency transmissions should be permitted on the clear data channel;

– security features for IMT-2000 should have minimal impact on the user service traffic capacity of the air interface.

8.2.2 Access related requirements

The following access related service requirements on security apply to IMT-2000:

– it should be very difficult for intruders to impersonate the IMT-2000 user or subscriber;

– it should be very difficult for intruders to impersonate an IMT-2000 service provider/network operator in communication with an IMT-2000 user, or in communication with another IMT-2000 service provider;

– it should be very difficult for intruders over an IMT-2000 radio interface intentionally to restrict the availability of services to an IMT-2000 user;

– it should be very difficult for intruders over an IMT-2000 radio interface to take over (hijack) a traffic channel already in use by an IMT-2000 user;

– it should be very difficult for intruders over an IMT-2000 radio interface to manipulate transmitted user or control information, and modify this information into information of their own choice;

– it should be very difficult for intruders to access, read or modify an IMT-2000 user's stored subscription information (possibly not directly radio interface related);

– IMT-2000 service provision should include mechanisms to prove the correctness and authenticity of transactions carried out with IMT-2000 users;

– it should be very difficult for an intruder to access or implant false commands in the IMT-2000 network signalling structure and related control functions.

8.2.3 Radio interface related requirements

The following requirements on security relating to the IMT-2000 radio interface(s) apply to IMT-2000:

– it should be very difficult to decipher the IMT-2000 user's communication over an IMT-2000 radio interface. This applies to any service information type (voice, text, data, etc.) or signalling information;

– it should be very difficult for intruders, by interception over an IMT-2000 radio interface, to physically locate the IMT-2000 user;

– it should be very difficult for intruders, by interception over an IMT-2000 radio interface, to identify the IMT-2000 user associated with a particular communication;

– it should be very difficult for intruders to intercept signalling or control information over an IMT-2000 radio interface.

8.2.4 Terminal related requirements

The following terminal related requirements on security apply to IMT-2000:

– it should be possible for the IMT-2000 service provider/network operator to identify an unauthorized or stolen IMT-2000 mobile terminal, and then record and prevent access to the services by this equipment;

– it should be possible for the IMT-2000 service provider/network operator to detect the existence of, and prevent access to the services by a cloned IMT-2000 mobile terminal;

– it should be very difficult for intruders to obtain IMT-2000 mobile terminal identities and, in particular, terminal authentication information from an IMT-2000 mobile terminal;

– it should be possible for the IMT-2000 network operator to detect and prevent the use of an IMT-2000 mobile terminal which is not type approved or accepted by the IMT-2000 network operator for use on his system;

– it should be possible for an IMT-2000 network operator to identify a faulty IMT-2000 mobile terminal, and then record and prevent the use of this equipment.

Note 1 – The use of an IMT-2000 mobile terminal identity for its authentication, for mobility management and for other purposes 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.

Note 2 – A cloned IMT-2000 mobile terminal is a mobile terminal having exactly the same mobile terminal identity and authentication key as those of the authorized IMT-2000 mobile terminal. A type approved IMT-2000 mobile terminal is a mobile terminal which is authorized to gain access to the network from the regulatory point of view.

8.2.5 User association related requirements

If the user association with the IMT-2000 mobile terminal is realized by a provision on the user side, e.g. the user identity module, the following user association related requirements on security apply to IMT-2000. The provision is *represented* by the UIM in the following description:

– it should be possible for the IMT-2000 service provider to identify stolen UIMs (they are stolen IMT-2000 mobile terminals if the UIM is integrated in the mobile terminals), and then record and prevent the use of these UIMs (mobile terminals);

– it should be possible for the IMT-2000 service provider to detect and prevent access to the services by cloned UIMs;

– it should be possible for the IMT-2000 service provider to indirectly or directly authenticate the human user of the UIM;

– it should be very difficult for intruders to illicitly read out the IMT-2000 user associated security information from a UIM;

– it should be very difficult for intruders to illicitly write the IMT-2000 user identity and its associated security information into a UIM.

If the user association with the IMT-2000 mobile terminal is realized by a network capability, e.g. voice recognition technique, the above requirements do not apply. Instead, the following requirement applies:

– it should be very difficult for intruders to pretend to be the IMT-2000 users;

– other requirements are for further study.

8.2.6 Network operational requirements

The following network operational related requirements on security apply to IMT-2000:

– the security to be provided by IMT-2000 should be adequately standardized to provide secure international interoperability and roaming. However, within the security mechanisms of IMT-2000, the maximum independence between the parties involved in the IMT-2000 operation should be allowed, as well as the maximum freedom for all parties to make their own security policies and mechanisms;

– the security mechanisms of IMT-2000 should require the least possible long-distance real-time signalling connections (e.g. in order to avoid international signalling connections at every location update or call when roaming).

8.2.7 Security management requirements

The following security management related requirements apply to IMT-2000:

– security keys and possible devices, such as the UIM, distributed to the IMT-2000 users should be easily and securely managed and updated;

– management of security keys within and between IMT-2000 service providers should be secure;

– the IMT-2000 service provider should have secure mechanisms to record events associated with IMT-2000 users or subscribers;

– it should be very difficult for intruders to impersonate an IMT-2000 service provider in communication with IMT-2000 network operators, and vice versa;

– the security mechanisms provided by IMT-2000 should have means for version management, and should be easy to update during the lifetime of IMT-2000.

8.3 Security provided by IMT-2000

8.3.1 Security features

This section describes the security features provided by IMT-2000. A security feature can be provided as an inherent part of the IMT-2000 service or as a specific IMT-2000 security service.

Security features generally have one of the following properties:

– preventive,

– reporting,

– limiting,

– restoring,

– deterrent.

The security features have been categorized into essential and optional features, and are also categorized into user related features and service provider related features.

User related security features are provided with a direct security advantage for the IMT-2000 users, while service provider related security features are provided for the IMT-2000 service providers to meet the requirements for the overall security of the system affecting the IMT-2000 users only indirectly.

Note 1 – These security features are all for further study. The eventual inclusion of the features will depend on the result of the threat and risk analysis given in Annex 2, and on future decisions related to the IMT-2000.

8.3.1.1 User related security features

8.3.1.1.1 Essential user related security features

The following essential user related security features are provided by IMT-2000:

– **Access control for subscription data**: A feature by which there are restrictions on access to the personal data of an IMT-2000 user or subscriber stored in the network.

– **Access control for service profile data**: A feature by which there are restrictions on access to the personal service profile of an IMT-2000 user or subscriber stored in the network.

– **User action authorization**: A feature by which the various actions of an IMT-2000 user have various degrees of restriction. It requires an IMT-2000 user to be authorized for his actions.

– **Terminal action authorization**: A feature by which the various actions allowed for an IMT-2000 mobile terminal have various degrees of restriction. It requires an IMT-2000 mobile terminal to be authorized for its actions.

– **User data confidentiality**: A feature by which the data of an IMT-2000 user are protected against disclosure over the IMT-2000 radio interface. The feature applies to voice, or any other type of user data.

– **Signalling information confidentiality**: A feature by which the signalling information is protected against disclosure over an IMT-2000 radio interface.

– **User identity confidentiality**: A feature by which the identity of an IMT-2000 user is protected against disclosure over an IMT-2000 radio interface.

– **User location confidentiality**: A feature by which the physical location of an IMT-2000 user is protected against disclosure over an IMT-2000 radio interface.

– **User identity authentication**: A feature by which the identity of an IMT-2000 user is verified to be the one claimed.

– **Terminal identity authentication**: A feature by which the identity of an IMT-2000 mobile terminal is verified to be the one claimed. It may effectively be implemented by the user identity authentication.

– **UIM holder verification**: A feature by which the human user of the UIM is authenticated. This feature only applies when the UIM is used for the user association with the IMT-2000 mobile terminals.

– **Transaction data integrity**: A feature by which the IMT-2000 user and service provider can have some assurance that the data transmitted from the other side in a transaction has not been modified over the channel.

– **User location integrity**: A feature by which the home IMT-2000 service provider, the visited IMT-2000 service provider and/or the IMT-2000 network operator can have some assurance that the IMT-2000 user location related information cannot be modified by intruders.

– **Terminal location integrity**: A feature by which the home IMT-2000 service provider, the visited IMT-2000 service provider and/or the IMT-2000 network operator can have some assurance that the IMT-2000 mobile terminal location related information cannot be modified by intruders. It may effectively be implemented by the user location integrity.

– **Secure distribution of IMT-2000 user identity and its associated security information**: A feature by which the IMT-2000 user identity and its associated security information can be securely distributed to the UIM by the home IMT-2000 service provider at the time of registration of the IMT-2000 user. This feature only applies when the UIM is used for the user association with the IMT-2000 mobile terminals **(possibly not directly related to the radio interface)**.

– **Secure distribution of IMT-2000 mobile terminal identity and its associated security information**: A feature by which the IMT-2000 mobile terminal identity and its associated security information can be securely distributed to the IMT-2000 mobile terminal, if they are assigned by the IMT-2000 terminal manager, or to the IMT-2000 terminal manager, if they are assigned by the terminal manufacturers, at the time of registration of the IMT-2000 mobile terminal **(possibly not directly related to the radio interface)**.

– **Protected DTMF**: A feature by which DTMF is protected against eavesdropping over the IMT-2000 radio interface(s), if DTMF is generated in the IMT-2000 mobile terminal.

8.3.1.1.2 Optional user related security features

The following optional user related security features may be provided by IMT-2000:

– **Service provider authentication**: A feature by which the identity of an IMT-2000 service provider is verified to be the one claimed.

– **Re-authentication of users**: A feature by which the identity of an IMT-2000 user is re-verified to be the one claimed. This feature may be invoked repeatedly or at any appropriate instant.

– **Re-authentication of terminals**: A feature by which the identity of an IMT-2000 mobile terminal is re-verified to be the one claimed. This feature may be invoked repeatedly or at any appropriate instant.

– **User event reports**: A feature by which the IMT-2000 user will receive warning announcements or indications at critical moments in the operation of IMT-2000 services (e.g. information about accumulated charges, that his communication is un-encrypted, etc.).

– **Subscriber access to service profile**: A feature by which the IMT-2000 subscriber has direct and limited access to the personal service profile of his associated users, by means of which he may be able to restrict access to services, etc.

8.3.1.2 Service provision related security features

8.3.1.2.1 Essential security features

The following essential IMT-2000 service provision related security features are furnished by IMT-2000:

– **Denial of access to the service by users**: A feature by which the IMT-2000 service provider denies access to service by a particular IMT-2000 user **(possibly not directly related to the radio interface)**.

– **Backup of subscription data**: A feature by which the IMT-2000 service provider can restore data relating to IMT-2000 users or subscribers upon failure **(possibly not directly related to the radio interface)**.

– **Network fraud/Abuse control**: A feature by which a network operator with whom an IMT-2000 service provider/terminal manager has a relationship is provided with data necessary for him to effect fraud and abuse control for his network **(possibly not directly related to the radio interface).**

8.3.1.2.2 Optional security features

The following optional IMT-2000 service provision related security features may be furnished by IMT-2000:

– **Event logging**: A feature by which the IMT-2000 service provider can log activities relating to an IMT-2000 user or subscriber **(possibly not directly related to the radio interface)**.

– **Denial of access to the service by mobile terminals**: A feature by which the IMT-2000 service provider/ IMT-2000 network operator may deny a particular IMT-2000 mobile terminal access to service **(possibly not directly related to the radio interface)**.

8.3.1.3 IMT-2000 security features related to generic telecommunications network operation

IMT-2000 security features related to generic telecommunications network operation are security features which from an overall IMT-2000 system perspective are judged to be important, but which may already be defined or will be defined in appropriate ITU-T Recommendations for generic telecommunications network operation.

8.3.2 Security mechanisms

While the security features indicate **what** security is provided, the security mechanisms indicate **how** the security is provided. The security mechanisms will be dealt with in the future Recommendation on IMT-2000 security procedures.

8.4 Security management

Security management is the control and distribution of security relevant information to various parties involved, e.g. users and systems, for protecting users and other parties involved of IMT-2000. It is used for reporting security-relevant events, which affects protection of parties involved.

Security management in the IMT-2000 network will be dealt with in the future Recommendations on IMT-2000 network management.

8.5 Security architecture and procedures

The implementation requirements for IMT-2000 security mechanisms as procedures between the different parties involved in IMT-2000 will be given in the future Recommendation on IMT-2000 security procedures.

8.6 Security algorithms

The future Recommendation on IMT-2000 security procedures will define the requirements placed on security algorithms.

ANNEX 1

Vocabulary

The following terms and definitions have been used in this Recommendation:

– **Security feature**: A feature that gives some assurance against one or several potential security threats.

– **Security mechanism**: A means of providing a security feature.

– **Security service**: A service realizing a particular security feature as a supplementary service.

– **Security architecture**: The architecture of parties and entities relevant to security, and the complete set of security procedures and information flows for the realization of security features.

– **Security management**: Handling of the network and service management aspects of security, including administrative, operational and maintenance issues.

– **Security policy**: A set of rules which define and constrain the types of security-relevant activities of entities and parties.

– **IMT-2000 user**: A person, entity or process actually using the IMT-2000 services. An IMT-2000 user is associated with a unique user identity.

– **IMT-2000 subscriber**: A legal person or entity associated with the IMT-2000 subscription and responsible for the charges incurred by his associated IMT-2000 users. An IMT-2000 subscriber may be responsible for several IMT-2000 users.

– **IMT-2000 service provider**: A legal person or entity responsible for providing IMT-2000 subscriptions to IMT-2000 subscribers.

– **IMT-2000 network operator**: A legal person or entity ultimately responsible for providing complete IMT-2000 network functionality to IMT-2000 users. Parts of the complete IMT-2000 network functionality may, however, be provided by other parties.

– **UPT user**: A user using UPT services.

– **UPT subscriber**: The subscriber associated with a UPT user. A UPT subscriber subscribes to a UPT service provider.

– **UPT service provider**: A legal person or entity responsible for providing UPT subscriptions to UPT subscribers.

– **Confidentiality**: A property by which information relating to an entity or party is not made available or disclosed to unauthorized individuals, entities or processes.

– **Authentication**: A property by which the correct identity of an entity or party is established with a required assurance.

– **Integrity**: A property by which the information contents of an object is prevented from being modified.

– **Authorization**: A property by which the access rights to resources are established and enforced.

– **Privacy**: The right of individuals to control or influence what information related to them may be collected or stored and by whom and to whom that information may be disclosed.

ANNEX 2

Threat and risk analysis

TABLE OF CONTENTS

		Page
1.	Introduction	19
2.	Methodology	19
3.	Identification of threats	19
	3.1 Intentional threats	19
	3.2 Accidental threats	20
	3.3 Administrative threats	20
4.	Evaluation of threats and risks involved	21
	4.1 Intentional threats	21
	4.2 Accidental threats	22
	4.3 Administrative threats	22
5.	Evaluation of countermeasures and costs involved	23
	5.1 Intentional threats	23
	5.2 Accidental threats	26
	5.3 Administrative threats	26

1. Introduction

This Annex gives a threat and risk analysis of the security aspects of IMT-2000.

2. Methodology

The methodology used in the threat analysis in this Annex is the following:

– **identification of the system scenario** and the involved parties (covered by § 6 of the main body of this Recommendation),

– **identification of the threats** and vulnerabilities of the system,

– **evaluation of the threats and the risks** associated with each threat,

– **evaluation of countermeasures and the cost**, and

– **definition of the detection, resistance and recovery mechanisms** needed to counter potential threats to maintain system security and integrity, with an assessment of their justification for implementation (covered by § 8.5 and 8.6 of the main body of this Recommendation).

3. Identification of threats

This section identifies the threats associated with the IMT-2000 service provision and use. Although the system assumptions relevant to security and the parties involved in the IMT-2000 service provision are given in § 9.1 and 9.2 of the main body of this Recommendation, the statements made in the following sections of this annex are not fully compliant with them. Rather, the statements below use to some extent simplified system architecture and generic terms.

Threats can be divided into the following general categories:

– intentional threats,

– accidental threats, and

– administrative threats.

3.1 Intentional threats

Intentional threats are those which are made by malicious intruders. They can further be classified into three categories.

3.1.1 Fraudulent use

3.1.1.1 Theft of mobile terminal

Once a mobile terminal, or user identity module if it is a physically detachable device, has been stolen by a thief, he will place fraudulent calls which the owner of the stolen mobile terminal or user identity module may be charged for, depending on the business policy of the service provider.

3.1.1.2 Theft of user credentials

3.1.1.2.1 Cloning

If a mobile terminal is temporarily exposed to dishonest persons (for instance, dishonest workers at a repair shop), the user-associated secret data which should be used to authenticate the user by the service provider/network operator during call set-up transactions may be read out and subsequently loaded into a fraudulent mobile terminal. This results in a clone of a legitimate mobile terminal which can be detected neither by the owner of the mobile terminal nor by the service providers/network operators usually until 30 days or more of fraudulent charges are incurred.

Such cloning may be exacerbated by the lack of security administration and management in the service provider/network operator.

3.1.1.2.2 Masquerading

If signalling takes place in plain text over the radio channel, an eavesdropper may listen to call set-up transactions, analyse them and deduce the secret data contained in the mobile terminal and/or the user identity module. He can subsequently pretend to be a legitimate user by emulating the correct call set-up transactions.

3.1.1.3 Hijacking

A hijacker could interrupt a call just after it has been set up but before the legitimate mobile terminal has begun conversation. This may also occur when a radio link is re-established during a call, such as in the handover operation in cellular telephone systems.

3.1.2 Threats to integrity

3.1.2.1 Coherent manipulation of users' data

The coherent manipulation of users' communication information is a threat in which the users' communication information is intentionally manipulated by the intruder so that it has a different meaning from what originally was, but still looks, meaningful for the users.

3.1.2.2 Malicious registration of location

Malicious registration of location is where an intruder intentionally attempts to register a legitimate user at a false location.

3.1.2.3 Malicious user service profile manipulation

Malicious user service profile manipulation is where there is an intentional attempt by the intruder to manipulate the service profile of a legitimate user or of all legitimate users. An example of manipulating all legitimate users' service profile is to implant a malicious virus into the database of the user service profile.

3.1.3 Threats to confidentiality, privacy and anonymity

3.1.3.1 Exposure of users' identities

The confidentiality of identities of the users, both calling and called parties, in communication is another area which is subject to threat.

3.1.3.2 Exposure of users' location

The confidentiality of the physical location of a user is another area which is subject to threat.

3.1.3.3 Eavesdropping on users' communication

As a nature of radiocommunication, conversation over the radio channel is vulnerable to attacks from eavesdroppers.

3.2 Accidental threats

Accidental threats are those which are caused by operational errors by the user, transmission errors and so on.

Further study is required to identify these threats.

3.3 Administrative threats

Administrative threats are those which are caused by the lack of security administration and management, the abuse of privileges and so on. Administrative threats are possibly not directly related to the radio interface.

3.3.1 Intrusion into the subscriber/user database

A subscriber/user database which contains the user-associated secret data usually requires provisions for audit, maintenance and backup, which makes it vulnerable to intruders. The intruder could be either an employee or a non-employee of the service provider/network operator. Intrusion into the subscriber/user database may result in cloning (see § 3.1.1.2.1).

3.3.2 Tapping of users' credentials in other networks

Where there is provision for national and international roaming, the possibility of having the secret data tapped when a user roams into a foreign network becomes a threat. The tapping of secret data may result in cloning (see § 3.1.1.2.1).

3.3.3 Intrusion into system database or network control functions

It may be possible for intruders to access and maliciously modify the database of the network control functions. It is also possible that an intruder may implant a malicious virus in the database of the network control functions.

4. Evaluation of threats and risks involved

4.1 Intentional threats

4.1.1 Fraudulent use

Fraudulent use results in economic damage to both users and service providers/network operators.

4.1.1.1 Theft of the mobile terminal

Theft usually results in economic damage to the user whose mobile terminal, or user identity module if it is a physically detachable device, has been stolen. However, the damage can be limited to the call charge that the user is liable for during the period between the theft and their report of the theft to the service provider/network operator. This is because the service provider/network operator can restrict calls to and from the mobile terminal once they receive such a report. The damage will therefore be rather small unless the user is not aware of the theft for a long time.

4.1.1.2 Theft of user credentials

4.1.1.2.1 Cloning

Cloning usually results in economic damage to the user of the legitimate mobile terminal, or user identity module if it is a physically detachable device. Cloning could also result in economic damage to the service provider/network operator, because this fraud tends to be undetected for a fairly long time, leading to a high probability of the victim user repudiating the unexpected bill.

The tendency of the cloning to be undetected for a long time could result in considerable economic damage to either or both the user or the service provider/network operator.

Cloning may also make the victim user unavailable for call termination, because the location registration by the clone mobile terminal may effectively work as a malicious registration of location (see § 3.1.2.2).

4.1.1.2.2 Masquerading

Masquerading usually results in economic damage to the user whose mobile terminal, or user identity module if it is a physically detachable device, has been emulated, and potentially to the service provider/network operator in a similar manner to the damage caused by cloning.

Masquerading may also make the victim user unavailable for call termination, because the location registration by the fraudulent mobile terminal may effectively work as a malicious registration of location (see § 3.1.2.2).

4.1.1.3 Hijacking

Hijacking usually results in economic damage to the victim user. However, because hijacking randomly attacks calls, and a single user therefore tends to be a one-time victim, the resulting damage would be fairly small from the individual user's point of view.

Hijacking would also potentially result in economic damage to the service provider/network operator, because the victim user would complain about the unexpected call interruption. If the service provider/network operator accepts the users' complaints, the economic damage to the service provider/network operator would become serious.

4.1.2 Threats to integrity

4.1.2.1 Coherent manipulation of users' data

The coherent manipulation of users' communication information results in the victim users receiving false messages, thus leading to damages or inconvenience to the victim users. The degree of damage or inconvenience would vary on a case-by-case basis. This threat cannot easily be detected.

4.1.2.2 Malicious registration of location

A malicious registration of location results in the unavailability of call termination, thus leading to damages or inconvenience to the victim users. The degree of damage or inconvenience would vary on a case-by-case basis.

4.1.2.3 Malicious user service profile manipulation

A malicious user service profile manipulation results in the unavailability of certain services, thus leading to damages or inconvenience to the victim users. The degree of damage or inconvenience would vary on a case-by-case basis. Intrusion into the user service profile database, such as by implanting a malicious virus, may damage the whole network associated with the attacked service provider.

4.1.3 Threats to confidentiality, privacy and anonymity

4.1.3.1 Exposure of users' identities

The exposure of identities of the users in communication, both calling and called parties, can result in the victim users being put at an unidentifiable risk.

4.1.3.2 Exposure of users' location

The exposure of physical locations of the users gives the intruder and other users an opportunity to track the victim users and therefore can result in the victim users being put at an unidentifiable risk.

4.1.3.3 Eavesdropping on users' communication

The degree of damage or inconvenience caused by eavesdropping on user's conversation results in the victim users being put at an unidentifiable risk. If the usage is for business, the risk of economic espionage could be very large. If the user is a public or political figure, the risk of economic damage and national security as a result of compromised privacy also could be very large.

4.2 Accidental threats

Further study is required to identify these threats, before the threats and associated risks can be evaluated.

4.3 Administrative threats

4.3.1 Intrusion into the subscriber/user database

Intrusion into the subscriber/user database results in an opportunity for the intruder to make a clone. Therefore, the risks identified for cloning apply (see § 4.1.1.2.1).

The intrusion also allows the intruder to obtain or manipulate the subscriber/user profile, which threatens the victim subscriber/user's privacy, and may cause susbstantial damages or inconvenience to the victim subscriber/user. Intrusion into a subscriber/user database may collapse an IMT-2000 network.

4.3.2 Tapping of users' credentials in other networks

Tapping of the subscribers'/users' credentials results in an opportunity for the tapper to make a clone. Therefore, the risks identified for cloning apply (see § 4.1.1.2.1).

4.3.3 Intrusion into system database or network control functions

Intrusion into the system database or network control functions may result in unexpected anomalies in the network operation, damage the integrity of the network, and could collapse the whole network.

5. Evaluation of countermeasures and costs involved

5.1 Intentional threats

5.1.1 Fraudulent use

5.1.1.1 Theft of mobile terminal

The owner of the stolen mobile terminal or user identity module may be protected from fraudulent calls in two ways.

a) *Access restriction upon report of theft*

This countermeasure is similar to the usual practice adopted for credit cards. That is, once the theft is reported to the service provider/network operator, they immediately register the fact in the subscriber database in order to reject subsequent fraudulent call attempts. Thus, the owner's liability is limited.

b) *User authentication*

This countermeasure implements a function in the mobile terminals or in the IMT-2000 network to authenticate the identity of the "user" (as opposed to authentication of the mobile terminal or user identity module). User authentication is not necessary between the user and the service provider/network operator.

The most commonly used method so far is the use of a PIN which should only be known to the legitimate owner of the mobile terminals or the user identity module. An example is the "electronic lock" used in cellular telephone services, where the process is completely executed within the mobile terminal.

5.1.1.2 Theft of user credentials

5.1.1.2.1 Cloning

a) *Use of a specially designed device*

One of the possible countermeasures to prevent dishonest persons from making clones is to use a specially designed device, so that the user-associated secret data is difficult to read out. This provision is most important if the user identity module is a physically integrated component of mobile terminals.

b) *Use of a physically detachable device*

The second possible countermeasure is to use a user identity module which is physically detachable from a host mobile terminal, i.e. to hold the user-associated secret data in a device which is seldom handed over to other users by the owner. An example of such a device is a smart card (IC card) which is inserted into mobile units when they are used.

c) *Service provider/network operator authentication*

The two solutions described in § 5.1.1.2.1 a) and b) will be augmented by implementing the service provider/network operator authentication feature, where the user identity module does not respond to invocations by the network without the successful authentication of the service provider/network operator. This prevents the intruder from attempting to obtain the user-associated secret data by crypto-analysis based on numbers of challenge/response pairs.

d) *One-time disposable key*

Another possible countermeasure for fraudulent use by cloning is to implement a one-time disposable key for use in user authentication during the call set-up process. The key is updated at each call attempt and stored both in the user identity module and the service provider/network operator. By this scheme, a clone can never work if the legitimate mobile unit places a call prior to the clone attempting a call, because the authentication of the legitimate user leads to registering a new key that is not known to the clones. On the other hand, the legitimate user cannot place a call if the clone successfully makes a call prior to the legitimate user attempting a call. The latter scenario provides the legitimate owner of the mobile terminal or detachable user identity module with an indication of the existence of the clone in a short period.

This method, however, has a problem associated with keeping call counters aligned between the user identity module and the service operator/network operator under a relatively unreliable radiocommunications environment.

e) *User authentication by service provider*

The "user" authentication (as opposed to authentication of the mobile terminal or user identity module) by the service provider prevents the clone placing a successful call unless it is used by the legitimate user. If the user authentication is made locally, the local user authentication should be associated with and correlated with the authentication of the mobile terminal/user identity module.

A reliable user authentication would require the user to input a long string of numbers or characters, leading to inconvenience for the users enjoying the service. The shorter the string is for user authentication, the weaker the degree of protection provided by this method would be.

A more user-friendly user authentication may be implemented in the future by means of the network capability such as use of voice recognition techniques.

f) *Detection of nearly simultaneous calls*

Although it is not a preventive measure against cloning, detection by the network of two simultaneous calls at the same user identity, or detection by the network of two nearly simultaneous calls at the same user identity but made from the locations geographically far apart from each other, will assist the service provider/network operator to be aware of the existence of a clone in a short time.

g) *Enhanced protection against administrative threats*

Enhancing the countermeasures for administrative threats reduces the chance of cloning (see § 5.3).

5.1.1.2.2 Masquerading

a) *Use of a cryptosystem on signalling transactions over the radio channel*

The general defence against masquerading is to avoid message transactions over the radio channel in which the user-associated secret data are transmitted in plain text. One possible method is to employ encryption of the signals sent back and forth during call set-up procedures. The type of cryptosystem and the method of securely maintaining the keys adopted for this purpose are subject to further study.

b) *Authentication not exposing secret information*

Another possible countermeasure is to adopt a user authentication scheme in which the user-associated secret data are never transmitted in plain text form over the radio channel and in which the data of the authentication transaction always varies on a call-by-call basis.

A typical example of such authentication is the method used in Japan's Personal Digital Cellular (PDC) system and the GSM system, in which an authentication response is generated by a mobile terminal based on a disposable random number sent by the network. This is called a "challenge and response" method.

The effectiveness of the challenge and response type authentication against masquerading depends on the robustness of the cryptosystem used to generate the response.

5.1.1.3 Hijacking

5.1.1.3.1 Use of a cryptosystem on signalling transactions over the radio channel

Hijacking attempts can be thwarted by the use of encryption in the call control messages which are sent back and forth during the call. As in the case of masquerading, the type of cryptosystem and the method of safely maintaining the keys of the cryptosystem are subject to further study.

5.1.1.3.2 Repeated authentication during a call

Repeating authentication during the call may also prevent attackers from attempting hijacking. However, frequent authentication attempts may be caused by the intruder in order for him/her to perform the crypto-analysis for obtaining the user-associated secret data based on numbers of challenge/response pairs. Therefore, the frequency

of authentication needs to be carefully considered and user authentication accompanied by simultaneous service provider/network operator authentication may be desirable if repeated authentication is implemented (see § 5.1.1.2.1 c)).

5.1.1.3.3 Encryption of the conversation data

Another countermeasure to prevent hijackers from successfully attempting hijacking is to apply encryption to the conversation data, the keys of which are not known to the intruder, though this would be rather passive protection. With this provision, the hijacker cannot obtain a transparent communication link for use if the hijacking takes place after the key exchange for encryption has been completed.

5.1.2 Threats to integrity

5.1.2.1 Coherent manipulation of users' data

5.1.2.1.1 Addition of a signature to user's data

In general, protection against the coherent manipulation is achieved by adding a "signature" to users' data. Either the "secret key encryption" or "public key encryption" algorithms can be used for generating the signature. In the case of contiguous real-time data transmission such as the speech conversation, adding the signature may be impractical because of the increased processing complexity and applying a cryptosystem with keys unknown to the intruder and other users would be more appropriate. The use of encryption will also make conscious manipulation impossible.

5.1.2.1.2 Repeated authentication during a call

Repeated authentication during a call could be an alternative countermeasure to the protection approach described in § 5.1.2.1.1 above. The caution described in § 5.1.1.3.2 for repeated authentication should be noted.

5.1.2.2 Malicious registration of location

5.1.2.2.1 Authentication in every location registration transaction

In general, protection against malicious registration of location is provided by performing authentication in each transaction of location registration.

5.1.2.2.2 Use of a cryptosystem on location registration transactions

Applying a cryptosystem to location registration transactions is another countermeasure, subject to the availability of a secure method for key exchange.

5.1.2.2.3 Location registration at each call origination

Performing the location registration whenever an authenticated call origination is attempted will reduce the user damages caused by malicious registration of location, though this is not a preventive measure.

5.1.2.3 Malicious user service profile manipulation

5.1.2.3.1 Authentication in every manipulation transaction

In general, protection against malicious user service profile manipulation is provided by performing authentication in each transaction of the user service profile manipulation.

5.1.2.3.2 Use of a cryptosystem on manipulation transactions

Applying a cryptosystem to transactions of the user service profile manipulation is another countermeasure, subject to the availability of a secure method for key exchange.

5.1.3 Threats to confidentiality, privacy and anonymity

5.1.3.1 Exposure of users' identities

5.1.3.1.1 Use of a cryptosystem on identities

A possible countermeasure to maintain the confidentiality of users' identities is to apply a cryptosystem to the identities in the call control messages.

5.1.3.1.2 Use of temporary user identities

Another countermeasure is to employ temporary user identities which are only valid during a limited period.

5.1.3.2 Exposure of users' location

5.1.3.2.1 Use of a cryptosystem on identities

One possible countermeasure to maintain the confidentiality of users' locations is to apply a cryptosystem to the user identity in location registration messages.

5.1.3.2.2 Use of temporary user identities

Another countermeasure is to employ temporary user identities which are only valid during a limited period.

5.1.3.3 Eavesdropping on users' communication

5.1.3.3.1 Use of cryptosystem

Protection against the eavesdropping is achieved by employing a cryptosystem in the user communication channels. A variety of cryptosystems and a variety of methods of key distribution have been developed. By either the "secret key exchange algorithm" or the "public key exchange algorithm", key exchange can be achieved as a part of the user authentication transaction.

5.2 Accidental threats

Further study is required to identify these threats, before their costs and countermeasures can be evaluated.

5.3 Administrative threats

5.3.1 Intrusion into the subscriber/user database

Intrusion into the subscriber/user database is difficult to deal with.

5.3.1.1 Regulation of access

A minimum protection against this threat is to limit the access to the database to a minimum number of employees as well as to prohibit access by non-employees.

5.3.1.2 Ciphering stored data in database

Ciphering the stored data using a master key will enhance the security, though securely maintaining the master key requires another arrangement. A "public key exchange" method eliminates the need for the pre-user secret information exchange. This method needs to receive serious study.

5.3.2 Tapping of users' credentials in other networks

5.3.2.1 Prohibiting transfer of user-associated secret data

Protection against this threat could involve not permitting the users' secret data to be sent to foreign networks. This implies that a visited service provider/network operator has to request a set of non-secret information for the authentication and/or the encryption from the home service provider/network operator at every transaction related to the call set-up or the location registration.

5.3.3 Intrusion into system database or network control functions

5.3.3.1 Isolation of system database or network control functions from public networks

A promising method for protection against intrusion into the system database or network control functions is to isolate them from the public telecommunications networks. However, this extremely limits the maintainability of the network elements such as radio base stations which are distributed at geographically different locations.

5.3.3.2 Authorization and authentication of access to system database or network control functions

When the network elements having control functions and the database can be remotely accessed, via public telecommunications networks, access should be limited to authorized persons and to specific functions depending on the person. The person who accesses the network should always be authenticated by the network element.

ANNEX 3

Security procedures

This Annex outlines the kind of security procedures that may be foreseen for inclusion in the future Recommendation on IMT-2000 security procedures. These procedures include the following potential issues:

- elementary security procedures:
  - user and terminal identity confidentiality over the radio interface,
  - user and terminal identity confidentiality over the service provider – network operator interface,
  - user authentication,
  - terminal authentication,
  - encryption;
- security procedures during location updating:
  - initial location updating,
  - location updating within an IMT-2000 network operator's area,
  - location updating over the boundary of different IMT-2000 network operators' areas;
- security procedures during call set-up:
  - incoming IMT-2000 call,
  - outgoing IMT-2000 call;
- security procedures during calls:
  - security procedures during handover,
  - security procedures during in-call modifications;
- security procedures during call release:
  - call release;
- security procedures related to specific security services:
  - periodic authentication,
  - authentication by the home IMT-2000 service provider,
  - authentication by the IMT-2000 network operator.