

RECOMMENDATION ITU-R M.1223

EVALUATION OF SECURITY MECHANISMS FOR IMT-2000*

(Question ITU-R 39/8)

(1997)

CONTENTS

	<i>Page</i>
1 Introduction	182
2 Scope	183
3 Structure of the Recommendation	183
4 Related documents	183
5 Definitions	183
6 Considerations	184
7 Recommendation	185
7.1 Requirements on security mechanisms	185
7.2 Classes of security mechanisms	185
7.2.1 Authentication mechanisms	185
7.2.1.1 Symmetric key	185
7.2.1.2 Asymmetric key	186
7.2.1.3 Zero knowledge	187
7.2.2 Anonymity mechanisms	187
7.2.2.1 Temporary identities using symmetric key	187
7.2.2.2 Identity confidentiality using asymmetric key	187
7.2.2.3 Anonymous access	188
7.2.3 Confidentiality mechanisms	188
7.2.3.1 Block ciphers	188
7.2.3.2 Stream ciphers	188
7.2.4 Non-cryptographic security mechanisms	188
7.2.4.1 User verification	188
7.2.4.2 Registration	189
7.2.4.3 Call count	189
7.2.5 Integrity mechanisms	189
7.2.5.1 Encipherment	189
7.2.5.2 Symmetric key	190
7.2.5.3 Asymmetric key	190
7.2.6 Non-repudiation mechanisms	190
7.2.7 Security management	190
7.2.7.1 Key management	190
7.2.7.2 Version management	190
Annex 1 – Candidate security mechanisms	191
1 Mutual authentication mechanism based on a secret key check function	191
1.1 Features provided	191
1.2 Initial requirements	191
1.3 Mechanism description	192
1.3.1 Current registrations	192
1.3.2 New registrations	192

* International Mobile Telecommunications-2000 (IMT-2000) is also known as Future Public Land Mobile Telecommunication Systems (FPLMTS).

	<i>Page</i>
1.4 Evaluation	193
1.4.1 Security service provision	193
1.4.2 Communications overheads	194
1.4.3 Administration overheads	194
1.4.4 Processing and other hardware overheads	194
1.4.5 Adherence to international standards	194
1.4.6 Limitations on use	194
2 Unilateral authentication mechanism based on digital signatures	194
2.1 Features provided	194
2.2 Initial requirements	194
2.3 Mechanism description	195
2.3.1 Current registrations	195
2.3.2 New registrations	195
2.4 Evaluation	196
2.4.1 Security service provision	196
2.4.2 Communications overheads	196
2.4.3 Administration overheads	196
2.4.4 Processing and other hardware overheads	196
2.4.5 Adherence to international standards	196
2.4.6 Limitations on use	196
3 Unilateral authentication mechanism based on public key schemes	196
3.1 Features provided	197
3.2 Initial requirements	197
3.3 Mechanism description	197
3.3.1 Public key certificates	198
3.3.2 The authentication mechanism	198
3.3.3 A variant	198
3.4 Evaluation	198
3.4.1 Security service provision	198
3.4.2 Communications overheads	199
3.4.3 Administration overheads	199
3.4.4 Processing and other hardware overheads	199
3.4.5 Adherence to international standards	199
3.4.6 Limitations on use	199

1 Introduction

International Mobile Telecommunications-2000 (IMT-2000), also known as Future Public Land Mobile Telecommunication Systems (FPLMTS), are third generation mobile systems that 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 specific to mobile users.

A range of mobile terminal types is encompassed, accessing terrestrial or satellite-based networks, with terminals being 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 fixed networks,

- high quality,
- use of a small pocket-terminal with worldwide roaming capability,
- low cost.

IMT-2000 are defined by a set of interdependent ITU Recommendations of which this one 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 security measures to prevent transmitted data from being accessed by unauthorized parties. In addition, the nature of mobile communication requires security measures to prevent fraudulent access to services, and misappropriation of provider and operator resources.

2 Scope

The scope of this Recommendation is to identify classes of security mechanisms appropriate for implementing the IMT-2000 security features defined in Recommendation ITU-R M.1078 on security principles for FPLMTS, and thus for satisfying the FPLMTS security requirements identified in the same Recommendation. Annex 1 to this Recommendation describes specific candidate security mechanisms, and assesses their suitability for use in IMT-2000/FPLMTS.

This Recommendation is intended to be a starting point for the development of more detailed IMT-2000 Recommendations relevant to security which will be developed by various ITU Study Groups.

3 Structure of the Recommendation

A number of requirements on security mechanisms are identified in § 7.1. Section 7.2 identifies various classes of security mechanisms, and discusses their suitability for implementing the IMT-2000 security features identified in Recommendation ITU-R M.1078. In Annex 1, several candidate security mechanisms for IMT-2000 are described, and their suitability assessed.

4 Related documents

The following ITU Recommendations contain information on IMT-2000/FPLMTS relating to this Recommendation:

Recommendation ITU-R M.687:	Future Public Land Mobile Telecommunication Systems;
Recommendation ITU-R M.1078:	Security principles for Future Public Land Mobile Telecommunication Systems (FPLMTS);
ITU-T Recommendation F.115:	Service objectives and principles for Future Public Land Mobile Telecommunication Systems.

5 Definitions

The following acronyms are used in this Recommendation:

IMUI:	international mobile user identity
TMUI:	temporary mobile user identity
IMTI:	international mobile terminal identity
TMTI:	temporary mobile terminal identity
SPID:	service provider identity
NOID:	network operator identity

Knu:	user-network operator secret key (symmetric key schemes)
Ksu:	user-service provider secret key (symmetric key schemes)
Kpu:	user public verification key (asymmetric key schemes)
Ksign:	user private signature key (asymmetric key schemes)
Kss:	service provider private signature key (asymmetric key schemes)
Kps:	service provider public verification key (asymmetric key schemes)
Ksn:	network operator private deciphering key (asymmetric key schemes)
Kpn:	network operator public enciphering key (asymmetric key schemes)
Ks:	session key
Au:	user authentication algorithm
At:	terminal authentication algorithm
As:	service provider authentication algorithm
An:	network operator key generation algorithm
Ak:	session key generation algorithm
Cu:	identity hiding algorithm
E:	ciphering transformation (public key ciphering algorithm)
D:	deciphering transformation (public key ciphering algorithm)
S:	signing transformation (digital signature)
V:	verification transformation (digital signature)
H:	hash function
RND:	random authentication challenge
RES:	authentication check value
CERT:	certificate
CIPH:	a string of bits used to conceal identity
SIG:	signature
KO:	key offset

6 Considerations

In the development of 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) due to the particular nature of wireless communications, provision should be implemented in IMT-2000 for privacy of communication over the radio interface;
- e) due to the nature of mobile communication, concrete steps are required to prevent fraudulent access to services, and the misappropriation of provider and operator resources;
- f) system overview given in § 6 of Recommendation ITU-R M.1078;
- g) the relevant ITU-T and ITU-R Recommendations and ongoing studies;
- h) the need for a flexible system structure able to match network investment to 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.

7 Recommendation

Requirements on security mechanisms, and classes of security mechanisms that are recommended for IMT-2000 are given below.

7.1 Requirements on security mechanisms

- a) The security mechanisms should require the minimum of long-distance real-time signalling. For instance, the need for international signalling connections at every location update or call when roaming should be avoided.
- b) The security mechanisms should require a minimum of bilateral pre-arrangements between service providers and network operators.
- c) The security mechanisms should include the means to manage cryptographic keys which may need to be exchanged by service providers and network operators.
- d) The security mechanisms needed by users should be such that it is easy to distribute and change their cryptographic keys.
- e) The security mechanisms should be standardized only to the extent needed for interoperability and roaming.
- f) The security mechanisms should support version control management to allow for subsequent upgrading and revision of mechanisms.
- g) The security mechanisms should include the means to detect and report security violations, and the means to restore the system to a secure state.
- h) The security mechanisms should satisfy legal requirements imposed by national authorities e.g. export controls, lawful interception;
- j) The security mechanisms should allow independent handling of user-related security features and terminal-related security features in order that IMT-2000 be able to support both user mobility, wherever it is required, as well as terminal mobility.

7.2 Classes of security mechanisms

Whilst security features indicate what security is provided, security mechanisms indicate how the security is to be provided. This section identifies various classes of security mechanism, and discusses their suitability for providing the security features to be supported by IMT-2000. The classes identified are based on the classification used by ISO wherever possible. In addition, potential advantages and disadvantages of the various approaches are listed.

Only high level descriptions of mechanism classes are given here. More detailed descriptions of particular mechanisms are given in Annex 1. The classes of mechanisms are ordered according to the security feature they most appropriately fulfil.

The term "entity" will be used throughout to indicate an unspecified role (e.g. user, terminal, service provider, network operator, etc.).

7.2.1 Authentication mechanisms

A fundamental distinction among security mechanisms is that between so-called "symmetric" (or secret-key) mechanisms and "asymmetric" (or public-key) mechanisms. Symmetric key mechanisms have been successfully employed in existing mobile systems, asymmetric key mechanisms would be a novelty in mobile systems, but have been successfully employed in existing computer networks.

7.2.1.1 Symmetric key

In symmetric key mechanisms, each entity has an associated secret key. Keys are only available to the owning entity and entities trusted by the owner, and must be securely stored, possibly in a removable user identity module (UIM), e.g. smart card, or in a secured database. Authentication is based on the principle that the secret key of an entity only is known by itself and a limited number of trusted entities e.g. those who wish to authenticate the owner.

To obtain authentication, the entity to be authenticated must exhibit knowledge of the secret key to the authenticating party. This may be done through the generation of challenge – response pairs, perhaps by using the secret key as input (along with other data) to a one-way cryptographic algorithm.

Advantages:

- for authentication between user and network operator, the use of service provider specific algorithms may be possible. If the network operator is issued with pre-computed authentication parameters from the service provider then the authentication algorithm can be service provider specific. Alternatively, if the network operator receives a (temporary) authentication key, then the authentication key calculation algorithm can be service provider specific;
- can be easily adapted to calculate session keys;
- relatively simple and fast algorithms;
- small amount of data required for authentication.

Disadvantages:

- secured databases have to be available in the network;
- if the network operator receives a temporary authentication key, then a standardized authentication algorithm must be used across all networks and UIMs;
- it may be difficult to adapt the mechanisms to cater for authentication between arbitrary entities, due to the necessary distribution of secret keys;
- a trust relation must be present between the service provider and the network operators for the exchange of keys or pre-calculated authentication sets;
- a secure communication between the service provider and network operators is required;
- other features such as incontestable charging and user identity confidentiality may be more difficult to realize.

7.2.1.2 Asymmetric key

In asymmetric key mechanisms, each entity to be authenticated has a public key and corresponding secret key. The secret key is known only to the owner (e.g. user or network component), whilst the public key may be distributed.

Authentication is achieved by the claimant exhibiting knowledge of the appropriate secret key to the authenticating entity. Authentication generally works as follows: to provide authentication, the claimant uses his secret key to calculate appropriate authentication information from specified authentication input data. The verifier can then use the corresponding public key for verification.

A number of approaches are available for distribution of the public key. For example, an entity may possess a certificate, calculated by a trusted entity, that certifies the authenticity of the public key. This certificate can then be distributed as required. Alternatively, a database in the network may be available, containing certificates for all entities. Both of these approaches require the availability of a further trusted entity, to calculate certificates or manage the database. Another alternative is to pre-install public keys of potential communication partners within an entity.

Advantages:

- no need to store or transmit secret authentication keys within a network;
- signalling to the service provider may be unnecessary;
- easily adapted for authentication between any pair of entities;
- secure communication between service provider and network operators is not necessary.

Disadvantages:

- the authentication algorithms generally have a greater computation complexity;
- fewer candidate algorithms are available;
- the authentication algorithm has to be agreed on worldwide basis, although the use of several negotiable versions is possible;
- message exchanges tend to be longer;
- certification authorities may be required.