RECOMMENDATION ITU-R M.1223

EVALUATION OF SECURITY MECHANISMS FOR IMT-2000

(Question ITU-R 39/8)

(1997)

CONTENTS

Page

1 Introduction

International Mobile Telecommunications-2000 (IMT-2000) 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 IMT-2000, and thus for satisfying the IMT-2000 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.

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-20001 relating to this Recommendation:

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

Recommendation ITU-R M.1078: Security principles for International Mobile Telecommunications-2000 (IMT-2000);

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)
Ksigu: 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.

7.2.1.3 Zero knowledge

With this approach, the user has two identities, a public identity (PI) and a corresponding secret identity (SI). These identities are constructed by the service provider and written to the UIM. To construct the identities requires knowledge of some secret parameters (e.g. the factors of some large integer *N*), but the relationship between the identities can be verified using a parameter which does not need to be protected against disclosure (e.g. the integer *N* itself).

Verification of an entity's identity uses a zero-knowledge protocol, which enables the verifier to be convinced that the entity knows the secret identity without the verifier (or any eavesdropper) gaining any knowledge of this identity – even if the verifier abuses the protocol.

Advantage:

– adjustable level of security.

Disadvantages:

– mechanisms tend to be complex;

– session key agreement/distribution cannot be easily integrated;

– large amounts of data must be transmitted.

7.2.2 Anonymity mechanisms

7.2.2.1 Temporary identities using symmetric key

A temporary identity is disposable and only valid during a limited period of time. A temporary identity may be unique only in a location area, and may for example, be re-allocated at every location update.

The temporary identity can be used on every insecure link for identification purposes, guaranteeing the entities anonymity. The assignment of the temporary identity has to be secured, e.g. by encryption. For some mechanisms, in exceptional cases the use of the permanent identity can be allowed.

Advantage:

– temporary identities are shorter.

Disadvantages:

– assignment of temporary identities may require some supplementary management to avoid duplication;

– when errors occur the permanent identity may have to be used.

7.2.2.2 Identity confidentiality using asymmetric key

Entity identity confidentiality could also be provided by using a public key cryptosystem.

The entity may expand its permanent identity (e.g. with a random number), and then encipher this using a public key algorithm (e.g. Rivest-Shamir-Adleman (RSA)) with the public key of the receiving party, e.g. network operator, service provider or user.

The expansion is needed to prevent intruders from recreating the encrypted identity, and thus verifying the identity.

Advantages:

– no temporary identities are required;

– the identity never has to be sent unprotected.

Disadvantage:

– enciphered identities (using asymmetric algorithms) are longer than the plain-text identity.

7.2.2.3 Anonymous access

Mechanisms not making use of any identification could also be considered to achieve anonymity, e.g. use of pre-paid card.

Advantage:

– the risk of disclosing identities is completely removed.

Disadvantage:

– scenarios where anonymous access is allowed are rare.

7.2.3 Confidentiality mechanisms

Confidentiality mechanism could use a stream cipher or a block cipher. The ciphering function normally resides in IMT-2000 mobile terminals.

– more than one algorithm may need to exist to satisfy various legal/national policy constraints;

– for roaming purpose, some degree of standardization will be necessary.

7.2.3.1 Block ciphers

Block ciphers are characterized by the encipherment of fixed length field data under control of a key. Normally, block ciphers are used in an appropriate mode of operation such as the ECB, CBC, CFB and OFB mode (refer to ISO/IEC 10116, "Modes of operation for *n*-bit block cipher algorithm," 1991).

Advantage:

– block ciphers are normally well documented.

Disadvantages:

– some error propagation may occur;

– delays in decryption are unavoidable.

7.2.3.2 Stream ciphers

A stream cipher is a system whereby a key is fed into a sequence generator which uses the key to generate a sequence of arbitrary length. This key stream is then added to the data on a bit-by-bit basis.

Advantage:

– errors not usually propagated.

7.2.4 Non-cryptographic security mechanisms

7.2.4.1 User verification

Verification mechanisms check if the current user is the genuine user of the UIM or at least trusted by the genuine user. If the UIM is removable from the terminal, the terminal may also verify the user. Two methods are often used: one way protocol and a challenge/response protocol. Generally, there is a trade-off between the amount of efforts required by the user and the degree of security achieved.

A typical one way protocol for user verification is the utilization of a personal identity number (PIN) which is a secret number known only to the owner (or other authorized entity) of the terminal/UIM and the terminal/UIM itself. The user is required to enter the PIN via the keypad. The PIN is then checked in the terminal/UIM.

A typical method of challenge-response protocol for user verification is an interaction where the terminal/UIM generates a random number of a few digits and the user gives the result of a simple calculation on it, which the terminal/UIM can check.

Advantage:

– no network interaction required.

Disadvantage:

– human interaction is required, thus only very weak authentication mechanisms can be used.

7.2.4.2 Registration

Each type-approved terminal has a unique terminal identity. The network may interrogate the terminal and request the identity. Alternatively, the identity may accompany other data sent during particular procedures. The network stores databases containing lists of unique terminal identities. The database may comprise a number of different lists: white list, grey list and black list. The black list contains identities of terminals that are no longer authorized to use the network. The grey list contains identities of suspect terminals. The white list contains authorized identities.

Individual networks can decide whether they provide such databases. Central databases are necessary, containing all (internationally) available terminals and their associated status, to allow complete interworking and international roaming.

Advantage:

– can be used to identify a number of different equipment problems e.g. stolen, malfunctioning, and non-type approved.

Disadvantages:

– an identity can be changed and predicted, it is not a protection against cloned terminals;

– regular updates (also internationally) are needed to have reliable information;

– extra signalling messages are required.

7.2.4.3 Call count

One form of clone detection is a “call count” parameter that may be updated in the UIM upon a command from the network. A similar counter will also be updated by the home service provider. If a particular UIM appears to have discontinuous values of “count”, there is a likelihood that a clone is masquerading as the legitimate UIM and may have accessed service prior to accesses by the legitimate user. This mechanism only detects UIM cloning.

A “call count” could also be linked to the terminal and updated in the terminal and in a global database, containing terminal identities and the associated call counts. This variant detects terminal cloning.

Advantage:

– no expensive physical protection mechanisms are required.

Disadvantages:

– management of the call count may be necessary in the network;

– extra signalling messages may be required.

7.2.5 Integrity mechanisms

7.2.5.1 Encipherment

If the transferred data contains suitable redundancy, then encipherment could provide enough assurance that the transmitted data has not been modified.

Advantage:

– no extra cost than the provision of confidentiality.

Disadvantages:

– no prevention from attacks based on replay (random numbers or counters must be added);

– can only be used with highly redundant data.

7.2.5.2 Symmetric key

There are two basic techniques for achieving the integrity of a message: message authentication codes (MAC) comprising a data string, which is a cryptographic function of the message and a secret key; manipulation detection code (MDC) comprising a data string which is only a function of the message. Due to the fact that the MDC generating function is publicly known, it is necessary to encrypt at least the MDC.

Advantage:

– relatively simple algorithms.

Disadvantages:

– no protection from attacks based on replay (random number or counters must be added);

– secret keys of communication partners are required;

– only protects against attacks by third parties.

7.2.5.3 Asymmetric key

A hash value of the original message is signed with the secret key of the sender. This signature is appended to the transmitted message, and can be checked by any receiver, possessing the senders public key.

Advantage:

– any third party can verify the data.

Disadvantages:

– algorithms tend to have greater computational complexity;

– fewer candidate algorithms are available.

7.2.6 Non-repudiation mechanisms

Digital signatures, calculated on known data, can be used to achieve non-repudiation of sent and received data.

Different levels of non-repudiation can be achieved according to the amount of data to be signed, how the calculated signatures and the original data are saved and stored.

Advantage:

– different levels of non-repudiation can be achieved.

Disadvantage:

– asymmetric algorithms have to be used to prevent the verifier from generating fake signatures.

7.2.7 Security management

7.2.7.1 Key management

Various forms of key generation, distribution, certification, etc. are available. The requirements for key management will be dependent upon the specific IMT-2000 mechanisms chosen to support IMT-2000 security features.

7.2.7.2 Version management

Version management is a mechanism which enables the system to update or replace the security procedures or mechanisms without the need to replace the existing IMT-2000 mobile terminals. One reason for having removable UIMs is to be able to update mechanisms and algorithms by issuing new UIMs (thereby leaving terminals unaffected).

ANNEX 1

Candidate security mechanisms

This Annex describes several examples of security mechanisms in detail without mapping onto the IMT-2000 functional architecture as stated in Recommendation ITU-R M.817. These security mechanisms are shown for illustrative purposes and other alternative mechanisms may also be applied.

1 Mutual authentication mechanism based on a secret key check function

This section describes an example of a mutual authentication mechanism based on the use of secret key cryptography and a challenge-response exchange. It combines the provision of user identity confidentiality, entity authentication and session key generation in a single mechanism.

1.1 Features provided

The mechanism provides the following security features:

– mutual entity authentication between the user and the network operator;

– user identity confidentiality over the communications path between the user and the network operator;

– session key establishment between the user and the network operator (for use in providing other security features, possibly including confidentiality and/or integrity for data passed between the user and network operator).

1.2 Initial requirements

The mechanism makes use of the following cryptographic algorithms:

– user authentication algorithm, Au. This algorithm takes as input a secret key and a data string and outputs a check value RES;

– service provider authentication algorithm, As. This algorithm takes as input a secret key and a data string and outputs a check value RES. This algorithm may be the same as or distinct from the algorithm Au;

– identity hiding algorithm, Cu. This algorithm takes as input a secret key and a data string and outputs a string CIPH used to conceal a user identity;

– session key generation algorithm, Ak. This algorithm takes as input a secret key and a data string and outputs a session key, Ks;

– network operator key generation algorithm, An. This algorithm takes as input a secret key and a data string and outputs a user-network operator secret key, Knu. This algorithm may be the same as or distinct from the algorithm Ak.

The mechanism makes use of the following types of cryptographic key:

– user-service provider secret key, Ksu. These are secret keys known only to a user and their service provider. These secret keys remain fixed for long periods of time;

– user-network operator secret key, Knu. These are secret keys known only to a user and their “current” network operator. These keys may remain fixed while a user is registered with a particular network operator. Associated with every such key is a key offset (KO), which is used in conjunction with the user-service provider secret key, Ksu to generate Knu;

– session key, Ks. These are secret keys also known only to the user and their current network operator (i.e. the network operator to whom they are registered). A new session key is generated as a result of every use of the authentication mechanism. These keys can be used for data encipherment, and/or for the provision of other security features.

The mechanism makes use of the following types of identifiers:

– international mobile user identity, IMUI. This is an identity permanently associated with a user. The IMUI is never passed across the air interface, thus preventing its unauthorized disclosure;

– network operator identity, NOID;

– temporary user identity for network operator, TMUIn. This (temporary) identity is used to identify a user to the network operator with which they are currently registered. It is known to the user and to the current IMT-2000 network operator;

– temporary user identity for service provider, TMUIs. This (temporary) identity is used to identify a user to its service provider. It is known to the user and to its service provider.

The mechanism has the following additional requirement:

– the network operator and service provider need a secure channel to exchange the second and third messages of the "new registration" version of the mechanism.

1.3 Mechanism description

There are two versions of the mechanism, depending on whether or not the user is currently registered with the network operator. We consider the two cases separately (although they are closely related).

1.3.1 Current registrations

We first consider the case where the user is already registered with the network operator. This means that the user and the network operator will share a valid temporary identity TMUIn and secret key Knu. The mechanism for this case consists of three messages exchanged between the user and the network operator. The service provider is not involved.

The three messages are as follows:

Message 1: User $\rightarrow$ NO: TMUIn, RNDu

Message 2: NO $\rightarrow$ user: RNDn, KO, TMUIn'+CIPHn, RESn

Message 3: User $\rightarrow$ NO: RESu.

It should be noted that + in the above messages means bit-by-bit binary addition of two strings.

The values RNDu and RNDn are random "challenges" generated by the user and the network operator respectively.

The values RESu and RESn are "challenge responses" generated by the user and the network operator respectively. RESn is calculated using the user authentication algorithm Au with key input Knu and data string input the concatenation of RNDn , RNDu and TMUIn'. RESu is calculated using the user authentication algorithm Au with key input Knu and data string input the concatenation of RNDu and RNDn.

TMUIn' is the "new" temporary user identity for use with the network operator. This will replace the current temporary identity TMUIn.

CIPHn is a string of bits used to conceal the new temporary identity TMUIn' whilst it is in transit between the network operator and the user. It is calculated using the identity hiding algorithm Cu with secret key input Knu and data string input RNDu.

The user and the network operator can compute a session key Ks as the output of the session key generation algorithm Ak when given secret key input Knu and data string input the concatenation of RNDu, RNDn and TMUIn'.

For the special case of user-to-network one-way authentication and identity hiding, the parameters RNDu and RESn would be not be utilized. In this special case, CIPHn is calculated using algorithm Cu with secret input Knu and data string input RNDn.

1.3.2 New registrations

We second consider the case where the user is not registered with the network operator. This means that the user and the network operator do not share any information. The mechanism for this case consist of five messages exchanged between the user, the network operator, and the service provider of the user.

The five messages are as follows:

Message 1: User → NO: TMUIs, RNDu

Message 2: NO → SP: TMUIs, RNDu

Message 3: SP → NO: TMUIs'+CIPHs, KO, Knu, RESs

Message 4: NO → user: TMUIs'+CIPHs, RESs, RNDn, KO, TMUIn'+CIPHn, RESn

Message 5: User → NO: RESu

First note that we assume that a secure channel is available for exchanging messages 2 and 3 between the network operator and service provider.

As previously, the values RNDu and RNDn are random "challenges" generated by the user and the network operator respectively.

The values RESu, RESn, and RESs are "challenge responses" generated by the user, network operator, and service provider respectively. RESn and RESu are calculated as in the previous case. RESs is calculated using the service provider authentication algorithm As with key input Ksu and data string input the concatenation of RNDu and TMUIs'.

TMUIs' is the "new" temporary user identity for use with the service provider. This will replace the current temporary identity TMUIs. As previously, TMUIn' is the "new" temporary user identity for use with the network operator.

CIPHs is a string of bits used to conceal the new temporary identity TMUIs' whilst it is in transit between the service provider and the user. It is calculated using the identity hiding algorithm Cu with secret key input Ksu and data string input RNDu. As previously, CIPHn is a string of bits used to conceal the new temporary identity TMUIn' whilst it is in transit between the network operator and the user.

On receipt of message 4, the user can compute the network operator secret key Knu as the output of the network operator key generation algorithm An, when given as secret key input Ksu, and data string input the key offset KO concatenated with the network operator identity NOID (this same calculation is done by the service provider on receipt of message 2).

As previously, the user and the network operator can compute a session key Ks as the output of the session key generation algorithm Ak when given secret key input Knu and data string input the concatenation of RNDu, RNDn and TMUIn'.

Note that, as a result of the above mechanism, the user and the network operator will share a secret key Knu and a temporary identity TMUIn'. Note also that, in the mechanism described here, the network operator is not automatically given the user's IMUI. If this is necessary for legal and/or operational reasons it can be included in the third message of the "new registration" authentication mechanism.

For the special case of user-to-network one-way authentication and identity hiding, the parameters RNDu and RESn would be not be utilized. In this special case, however, Steps 3 and 4 need to carry RNDs, random "challenge" generated by the service provider, in addition to those listed above. Furthermore, CIPHs is calculated using algorithm Cu with secret input Ksu and data string input RNDs, and CIPHn is calculated using algorithm Cu with secret input Knu and data string input RNDn.

1.4 Evaluation

The mechanism has the following significant characteristics.

1.4.1 Security service provision

The security mechanism appears to provide the services which it is designed to provide. Formal security proofs for the mechanism have been constructed. Constructing suitable check functions is a relatively straightforward procedure.

1.4.2 Communications overheads

The two versions of the scheme require three and five messages respectively. This is the minimum required for mutual authentication given that the service provider needs to be consulted and that timestamps are not used (the other two services are provided without requiring any additional messages). The messages will all be relatively short.

1.4.3 Administration overheads

The mechanism requires entities to store random challenges for short periods of time. Temporary identities and keys will also need to be stored. The service provider does need to be involved; however this involvement is restricted to occasions where a user wishes to make use of new network operator.

1.4.4 Processing and other hardware overheads

All the cryptographic algorithms can be made simple to compute.

1.4.5 Adherence to international standards

The three-pass version of the mechanism conforms to ISO/IEC 9798-4: 1995 (given that the elements of the messages are assembled in the correct order).

1.4.6 Limitations on use

The mechanism makes use only of check functions and does not use encipherment operations. Hence arranging for the transport of equipment implementing this mechanism across international frontiers is likely to be straightforward. There are no known patent licence restrictions.

2 Unilateral authentication mechanism based on digital signatures

This section describes an example of a unilateral authentication mechanism based on the use of a digital signature scheme and a challenge-response exchange. It combines the provision of user identity confidentiality and unilateral entity authentication in a single mechanism.

2.1 Features provided

The mechanism provides the following security features:

– unilateral entity authentication of the user to the network operator;

– user identity confidentiality over the communications path between the user and the network operator.

2.2 Initial requirements

The mechanism makes use of the following cryptographic algorithms:

– User digital signature algorithm. This algorithm will consist of two transformations, the signing transformation S, and the verification transformation V. The signing transformation will take as input a private signature key and a data string and outputs a signature SIG. The verification transformation will take as input a public verification key, a signature SIG, and a data string, and outputs a binary value (Yes/No) indicating whether or not the input SIG is a valid signature for the input data string.

The mechanism makes use of the following types of cryptographic key:

– user private signature key, Ksigu. These are private keys known only to a user. These private keys remain fixed for long periods of time. These keys will be used as input to the user signature transformation S;

– user public verification key, Kpu. These are public keys which may be known by many network operators. These keys will be used as input to the public verification transformation V.

The mechanism makes use of the following types of identifiers:

– international mobile user identity, IMUI. This is an identity permanently associated with a user. The IMUI is never passed across the air interface, thus preventing its unauthorized disclosure;

– temporary mobile user identity, TMUI. This (temporary) identity is used to identify a user to the network operator with which they are currently registered. It is known to the user and to the current IMT-2000 network operator.

2.3 Mechanism description

There are two versions of the mechanism, depending on whether or not the user is currently registered with the network operator. We consider the two cases separately.

2.3.1 Current registrations

We first consider the case where the user is already registered with the network operator. This means that the user and the network operator will share a valid temporary identity TMUI and the network operator will be equipped with a copy of the user public verification key Kpu. The mechanism for this case consists of three messages exchanged between the user and the network operator. The service provider is not involved.

The three messages are as follows:

Message 1: User → NO: TMUI

Message 2: NO → user: RNDn

Message 3: User → NO: RNDu, RESu.

The value RNDn is a random “challenge” generated by the network operator.

The value RNDu is a random number generated by the user.

The value RESu is a “challenge response” generated by the user. RESu is calculated using the signing transformation S with key input Ksigu and data string input the concatenation of RNDn and RNDu.

On receipt of the TMUI from the user, the network operator randomly generates the value RNDn and stores it for subsequent checking. The value RNDn is sent to the user as the second message of the mechanism.

On receipt of RNDn from the network operator, the user randomly generates the value RNDu. The values RNDn and RNDu are used to generate RESu, which is sent to the network operator in the third message of the mechanism.

On receipt of RESu the network operator uses it as the SIG input to the verification transformation V, with the concatenation of the stored value of RESn and the received RESu making up the data string input, and Kpu used as the key input. The output of V will be used to determine whether or not the user is valid.

2.3.2 New registrations

We second consider the case where the user is not registered with the network operator. This means that the user and the network operator do not share any information. The mechanism for this case remains to be specified. We note the requirements for this mechanism here.

– The user and network operator must be provided with a temporary user identity TMUI, to enable the user to identify itself to the network operator across the air interface without compromising the value of its IMUI.

– The network operator must be provided with a copy of the user public verification key Kpu.

Ideally these requirements should be met without necessitating the transmission of the user IMUI and/or a public key certificate for the user across the air interface (unless these values are enciphered in some way).

2.4 Evaluation

The mechanism has the following significant characteristics.

2.4.1 Security service provision

The security mechanism appears to provide the authentication service it is designed to provide. However, the provision of user identity confidentiality is less certain. The mechanism contains no provision for updating a TMUI; if the same TMUI is used repeatedly, then there is the possibility that an interceptor could link all the traffic belonging to one individual. This could partially compromise the identity confidentiality service.

There is also a problem with "initializing" the scheme. A method needs to be devised for dealing with new registrations. However, this is not an insuperable problem, and a new registration mechanism could be constructed using a variant of the scheme described in the next section.

A number of suitable digital signature algorithms exist. The presence of the second random number, Ru, within the scope of the calculation of RESu means that the user avoids providing the network operator with the signed version of a data string completely specified by the network operator. If the same signature key is used for signing other types of data, then this would be a security threat. If this threat does not exist then the random number RNDu could be made null, i.e. chosen to have length zero.

2.4.2 Communications overheads

The scheme requires three messages to be sent. In fact a *mutual* authentication mechanism using challenge-response can be devised with this number of messages, and, if initiated by the network operator, a unilateral authentication scheme requiring only two messages can easily be devised. The identity confidentiality service is provided without requiring any additional messages. The messages will all be relatively short with the exception of the third message; within that message the SIG field might typically contain between 512 and 1 024 bits.

2.4.3 Administration overheads

The mechanism requires entities to store random challenges for short periods of time. Temporary identities and keys will also need to be stored. The service provider does need to be involved; however this involvement is restricted to occasions where a user wishes to make use of new network operator.

The keys for the digital signature algorithm will typically be quite large (e.g. 1 024 bits or more) as compared with 64-128 bits for conventional algorithm.

2.4.4 Processing and other hardware overheads

The signature and verification computations may be relatively complex; the exact complexity will depend on the algorithm and the size of the keys used.

2.4.5 Adherence to international standards

The mechanism conforms to ISO/IEC 9798-3: 1993 (given that the elements of the messages are assembled in the correct order).

2.4.6 Limitations on use

The mechanism makes use only of a digital signature function and does not use encipherment operations. Hence arranging for the transport of equipment implementing this mechanism across international frontiers is likely to be straightforward. There are no known patent license restrictions on the mechanism itself, although some digital signature algorithms are the subject of patents.

3 Unilateral authentication mechanism based on public key schemes

This section describes an example of a unilateral authentication mechanism based on the use of a digital signature scheme, a public key encipherment scheme, public key certificates and timestamps. It combines the provision of user identity confidentiality and unilateral entity authentication in a single mechanism.

3.1 Features provided

The mechanism provides the following security features:

– unilateral entity authentication of the user to the network operator;

– user identity confidentiality over the communications path between the user and the network operator.

3.2 Initial requirements

The mechanism makes use of the following cryptographic algorithms:

– digital signature algorithm. This algorithm will consist of two transformations, the signing transformation S, and the verification transformation V. The signing transformation will take as input a private signature key and a data string and outputs a signature SIG. The verification transformation will take as input a public verification key, a signature SIG, and a data string, and outputs a binary value (Yes/No) indicating whether or not the input SIG is a valid signature for the input data string;

– public key encipherment algorithm. This algorithm will consist of two transformations, the enciphering transformation E, and the deciphering transformation D. The enciphering transformation will take as input a public enciphering key and a data string and outputs an enciphered data string. The deciphering transformation will take as input a private deciphering key and an enciphered data string, and outputs a clear text data string.

The mechanism makes use of the following types of cryptographic key:

– user private signature key, Ksigu. This is a private key known only to a user. These private keys remain fixed for long periods of time. These keys will be used as input to the signing transformation S;

– user public verification key Kpu. This is a public keys which is known by a user's service provider. These keys will be used as input to the verification transformation V;

– service provider private signature key, Kss. This is a private key known only to a service provider. These private keys remain fixed for long periods of time. These keys will be used as input to the signing transformation S;

– service provider public verification key, Kps. This is a public key known to all network operators having a service provision arrangement with a service provider. These keys will be used as input to the verification transformation V;

– network operator private deciphering key, Ksn. These are private keys known only to a network operator. These private keys remain fixed for long periods of time. These keys will be used as input to the public key deciphering transformation D;

– network operator public enciphering key, Kpn. These are public keys which are known by all users wishing to make use of a network operator. These keys will be used as input to the public key enciphering transformation E.

The mechanism makes use of the following types of identifiers:

– international mobile user identity, IMUI. This is an identity permanently associated with a user. The IMUI is never passed across the air interface, thus preventing its unauthorized disclosure;

– temporary mobile user identity, TMUI. This (temporary) identity is used to identify a user to the network operator with which they are currently registered. It is known to the user and to the current IMT-2000 network operator;

– service provider identity, SPID.

The mechanism has the following additional requirement:

– the users, network operators and service providers must all have synchronized clocks.

3.3 Mechanism description

There is only one version of the mechanism, which we now describe.

Unlike the previous case, this mechanism does not require the user to be already registered with the network operator. The mechanism for this case consists of one message sent from the user to the network operator. The service provider is not involved. However it does require a public key certificate to be conveyed from the service provider to the user at some initial time. We first describe the form of the certificate before going on to describe the mechanism itself.

3.3.1 Public key certificates

The certificate for a user, denoted CERTu, is the concatenation of the following data strings:

– the user's IMUI;

– the SPID;

– the time of issue;

– the lifetime of the certificate;

– the user public verification key Kpu;

– the output of the signing transformation S when given as input the private signature key of the service provider and data string equal to the concatenation of IMUI, SPID, the time of issue, the lifetime of the certificate, and Kpu.

The user can then supply the certificate to any network operator, who can use the certificate to obtain a verified copy of the user's public key, without any intervention from the user's service provider.

3.3.2 The authentication mechanism

The message sent from user to network operator is as follows:

– user $\rightarrow$ NO: AUTH

The value AUTH is the output of the public key enciphering transformation E when given as key input the network operator public enciphering key Kpn, and data string input the concatenation of the user certificate CERTu, a current timestamp Tu, and the value RESu.

The value RESu is calculated as the output of the signing transformation S when given as key input the user private signature key Ksigu, and data string input the timestamp Tu.

The timestamp Tu is generated from the user's clock.

On receipt of the AUTH from the user, the network operator first deciphers it using the public key deciphering transformation with the network operator private deciphering key Ksn. This will yield CERTu, Tu and RESu. The network operator now performs the following operations.

– The timestamp Tu is checked to see if it is current, i.e. within the "acceptance window".

– The network operator now uses the service provider public verification key Kps to verify the signature within the certificate. If the checks pass, then the certificate's validity period is also checked.

– Finally, the value RESu is input to the verification transformation (as the signature input), with data input the data string input the timestamp Tu and key input the user public verification key Kpu.

– If all checks pass and the verification transformation gives the output "Yes", then the user is accepted.

3.3.3 A variant

We next briefly note that once a user and a network operator have used the above mechanism, then it can be simplified by replacing CERT with TMUI (assuming the network operator will cache the user public verification key and the corresponding TMUI). This will save bandwidth and a verification operation by the network operator.

3.4 Evaluation

The mechanism has the following significant characteristics.

3.4.1 Security service provision

The security mechanism appears to provide authentication services it is designed to provide.

A number of suitable digital signature and public key encipherment algorithms exist.

3.4.2 Communications overheads

The scheme required that only one messages be sent. This is clearly the minimum required for unilateral authentication; the identity confidentiality service is provided without requiring any additional messages. The message will all be relatively long; the SIG field in the unenciphered string might typically contain between 512 and 1 024 bits, and the encipherment operation may expand the message further.

3.4.3 Administration overheads

The mechanism requires entities to store random challenges for short periods of time. Temporary identities will also need to be stored by users and network operators. The service provider does not need to be involved, except for issuing certificates to new users.

The keys for the asymmetric algorithms will typically be quite large (e.g. 1 024 bits or more) as compared with 64-128 bits for a conventional algorithm.

Users will need to store public encipherment keys for all network operators with which they might need to communicate. One might typically expect these keys to be distributed to a user by their service provider.

Network operators need to store the public verification keys for all service providers with which they have a service provision arrangement.

As already noted, there is a need for users, network operators and service providers to have access to synchronized clocks.

3.4.4 Processing and other hardware overheads

The signature and verification computations may be relatively complex; the exact complexity will depend on the algorithm and the size of the keys used. Similarly, the public key encipherment and decipherment operations may also be relatively complex.

3.4.5 Adherence to international standards

The mechanism may conform to ISO/IEC 9798-3: 1993 (given that the elements of the message are assembled in the correct order); it is not clear whether the standard permits authentication exchanges to be enciphered (this is a matter of interpretation).

3.4.6 Limitations on use

The mechanism makes use of a digital signature algorithm and a public key encipherment algorithm. Hence, because it incorporates an encipherment function, arranging for the transport of equipment implementing this mechanism across international frontiers could be less than straightforward. There are no known patent licence restrictions on the mechanism itself, although some digital signature algorithms and public key encipherment algorithms are the subject of patents.