Annex 8

"Security" Design Principle

Status of Issuing this Design Principle

IMT-2000 standard, which is currently being drafted as specification version 1, is targeted to finalize by April 1999. Security Algorithm standard is one of the items. How to proceed the study procedure for drafting Security Algorithm standard was discussed at the 2nd and 5th System WG meetings in 1998 to basically approve the following two procedures:

1) Security Algorithm standard
   Based on general documentation rules, each of Air, BS-MSC, MS-UIM, and [Abis] interfaces and specification of MS and BS should be separately documented for standardization.
   However, because the content of the Security Algorithm standard is limited, and because the Security Algorithm standard includes confidential matters even in the process of documentation, the Security Algorithm standard shall be documented in a separate volume.
2) Study procedure
   The matter shall be studied in two stages. In the Stage 1, the SDP AdHoc (Security Design Principle AdHoc) group is set up and it issues the security design principle. In the Stage 2, specifications including algorithms are drafted.
   The SDP AdHoc, which was positioned as an AdHoc under control of IMT-2000 Study Committee System WG and which was active from August 1998 to November 1998, documented this principle.

Target Security and Privacy Features

2.1 Scope of Standardization

The scope of standardization is shown below.
Note that, considering evolution from the 2nd generation to 3rd generation system, work is divided into Phase 1 and 2:

- Phase 1: Study security based on both GSM and ANSI because TTC is studying security flow based on both GSM- and ANSI-evolution approaches and because the connection to the existing core networks is considered to be important in ITU-T.
- Phase 2: The next phase, in which e.g. authentication using public key mechanism or version management of security data/mechanisms shall be used to consciously minimize the required effort.

(Description on symbols)
❍: Standardized; ∆: Standardized conditionally; X: Out of scope of standardization;
?: Whether or not there is any subject of standardization is not known

1) Phase 1

Table A8-1 Scope of Standardization in Phase 1

Item no.	Item	Mechanism	Algorithm	Key Generation Algorithm
1	User Identity Authentication	❍	Δ Note1	Δ Note1
2	Re-authentication of Users	❍	Δ Note1	Δ Note1
3	Network Operator / Service Provider Authentication	❍	Δ Note1	Δ Note1
4	User Data Confidentiality	❍	❍	Δ Note1
5	Signalling Information Confidentiality	❍	❍	Δ Note1
6	User Identity Confidentiality (temporary ID)	❍	X	X
7	User Location Confidentiality	❍	X	X
8	Access Control for Subscription and Service Profile Data	X	X	X
9	Version Control of Security Data and Mechanisms	❍ Note4	X	X
10	Writing subscriber data to UIM	Δ Note5	Δ Note5	Δ Note5
11	Emergency Call	❍ Note7	❍ Note7	❍ Note7

1) Phase 2

(Shaded parts in Table A8-2 mean items changed from Phase 1. This table shows the case where the version management of security data/mechanisms is conducted so that standardization is consciously minimized. In case of an authentication using public key mechanism, for example, classification may differ from one below.)

Table A8-2 Scope of Standardization in Phase 2

Item no.	Item	Mechanism (Information Flow Level)	Algorithm	Key Generation Algorithm
1	User Identity Authentication	X Note6	X Note6	X Note6
2	Re-authentication of Users	X Note6	X Note6	X Note6
3	Network Operator / Service Provider Authentication	X Note6	X Note6	X Note6
4	User Data Confidentiality	X Note6	X Note6	X Note6
5	Signalling Information Confidentiality	X Note6	X Note6	X Note6
6	User Identity Confidentiality (temporary ID)	X Note6	X	X
7	User Location Confidentiality	? Note2	? Note2	? Note2
8	Access Control for Subscription and Service Profile Data	? Note3	?	?
9	Version Control of Security Data and Mechanisms	❍ Note4	?	?
10	Writing subscriber data to UIM	Δ Note5	Δ Note5	Δ Note5
11	Emergency Call	❍	❍	❍

Note 1: This depends on UIM implementation (IC card/built-in type) and which system is the base.

Note 2: This item is not necessary if the user location confidentiality function can be enabled with air interface confidentiality and a temporary ID.

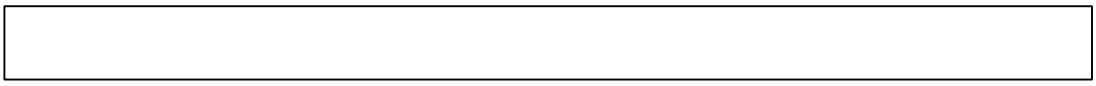
Note 3: This item is not necessary in cases where this function is defined as the data downloading function to UIM by OTA (Over the Air) and the function of accessing subscriber database due to activation, change or deactivation of supplementary services, because security can be guaranteed with the signalling information confidentiality on the air interface.

Note 4: In Phase 1, functions to provide the basic services are specified. In Phase 2, controlling the other security mechanism/algorithm is possible.

Note 5: Whether this is standardized or not depends on UIM implementation. (IC card/built-in type etc.) (Not standardized in case of IC card, while standardized in case of built-in type)
Note 6: There is no need for standardization if the version management function of security data and mechanisms is implemented.
Note 7: It is required to study the mechanism and algorithm of emergency call according to the UIM status.

Model Diagram

Overall Model Diagram

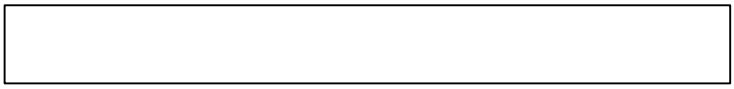


Note) UIM : User Identity Module, MS : Mobile Station, RAN : Radio Access Network,
CN : Core Network
H : Home, V : Visited (a visited network, including home network.)

Model for Data Writing to UIM/MS

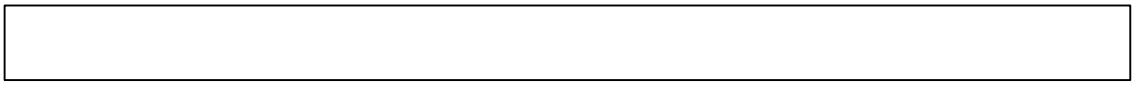
1) Removable UIM

[Basic 1] Data writing with writing device

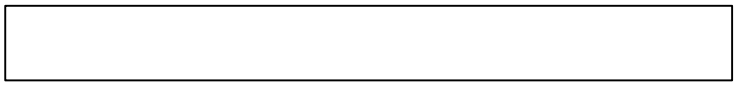


Note: In this model, the writing device is a dedicated device for each UIM.
The section between writing device and HLR shall not be subject to study.
HLR: Home Location Register

[Extended 1] Data writing with OTA

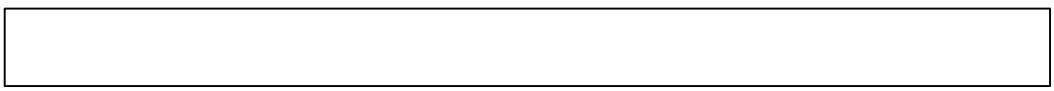


2) Non-Removable
[Basic 1] Data writing with writing device



Note: The section between writing device and HLR shall not be subject to study.

[Basic 2] Data writing with OTA



2.3 Authentication

2.3.1 User Identity Authentication

2.3.1.1 Authentication Algorithm

1) It is required to adopt a highly secure algorithm. (Key length and security against cryptanalysis should be also considered.)
2) Algorithm information shall not be disclosed at a roaming network, at the air interface or at a mobile terminal. An algorithm, which does not allow unauthorized access as long as an authentication key is not known even if the algorithm information is disclosed, is desirable.
3) An algorithm, which both hardware and software can process very fast (faster than allowed for authentication), regardless of the way UIM is implemented (IC card or built-in type), is desirable. For hardware implementation low complexity is desirable. For software implementation small program size and small memory requirements are desirable.

2.3.1.2 Key Generation Algorithm

1) It is desirable to adopt an algorithm, which can generate highly secure random number sequences with a longest possible period, i.e. occurrence of the same key should be minimized.
2) An algorithm, which both hardware and software can process very fast (faster than allowed for key generation), regardless of the way UIM is implemented (IC card or built-in type), is desirable. For hardware implementation low complexity is desirable. For software implementation small program size and small memory requirements are desirable.

2.3.2 Re-authentication of Users

2.3.2.1 Authentication Algorithm

See 2.3.1.1.

2.3.2.2 Key Generation Algorithm

See 2.3.1.2.

2.3.3 Network Operator / Service Provider Authentication

2.3.3.1 Authentication Algorithm

See 2.3.1.1.

2.3.3.2 Key Generation Algorithm

See 2.3.1.2.

2.4 Confidentiality

2.4.1 User Data Confidentiality

2.4.1.1 Encryption Algorithm

1) It is required to standardize an algorithm, which can be commonly adopted all over the world, in order to realize international roaming (Key length and security against cryptanalysis should be also considered). In addition, it is desirable to standardize another algorithm with higher security.
2) An algorithm, which both hardware and software can process very fast (faster than allowed for encryption and decryption), is desirable. For hardware implementation low complexity is desirable. For software implementation small program size and small memory requirements are desirable.

2.4.1.2 Key Generation Algorithm

1) It is desirable to adopt an algorithm, which can generate highly secure random number strings with a longest possible period, i.e. occurrence of the same key should be minimized.
2) An algorithm, which both hardware and software can process very fast (faster than allowed for key generation), regardless of the way UIM is implemented (IC card or built-in type), is desirable. For hardware implementation low complexity is desirable. For software implementation small program size and small memory requirements are desirable.

2.4.2 Signalling Information Confidentiality

2.4.2.1 Encryption Algorithm

See 2.4.1.1.

2.4.2.2 Key Generation Algorithm

See 2.4.1.2.

2.5 Data Writing to UIM/MS

2.5.1 Scope of Standardization for Security Functionality

Table A8-3 Scope of Standardization for Security Functionality

Function	UIM form	Method to write	Mechanism	Algorithm	Key generation algorithm
UIM/MS authentication (UIM administrator to UIM/MS)	Removable	Writing device	X	X	X
		OTA	O/X (note1, 4)	O/X (note 4)	O/X (note 4)
	Non-removable	Writing device	O	O	O
		OTA	O	O	O
UIM administrator (note2) authentication (UIM/MS to UIM administrator)	Removable	Writing device	X	X	X
		OTA	O/X (note1, 4)	O/X (note 4)	O/X (note 4)
	Non-removable	Writing device	O	O	O
		OTA	O	O	O
Air interface confidentiality (ciphering with UIM data being initialized)	Removable	OTA	O/- (note 3)	O/- (note 3)	X/- (note 3)
	Non-removable		O	O	O
UIM-to-writing device confidentiality	Removable	Writing device	X	X	X
	Non-removable		O	O	O
UIM-to-UIM administrator (note 2) confidentiality	Removable	Writing device	X	X	X
		OTA	X	X	X
	Non-removable	Writing device	-	-	-
		OTA	O	O	O
Stored data confidentiality	Removable	Writing device/OTA	X	X	X
	Non-removable	Writing device /OTA	X	X	X

O: Standardization; X: Out of scope of standardization; -: Not applicable

Note 1: This is not subject to standardization if the air interface procedure is implemented with a standardized procedure, e.g. GSM SIM Application Toolkit (using user information of SMS (Short Message Services)). If it is a dedicated procedure, it is subject to standardization.

Note 2: UIM administrator means a UIM provider/administrator including a network operator/service provider.

Note 3: No confidentiality is necessary if security is maintained only with UIM-to-UIM administrator confidentiality. This is subject to standardization in other cases.

Note 4: It dose not preclude applying contents standardized for Non-removable UIM to Removable UIM.

2.5.2 Security Functionality

2.5.2.1 Authentication

1) UIM/MS authentication

Functions to authorize writing-destination UIM/MS.

2) UIM administrator/writing device authentication
Functions to prevent illegal data writing by using unauthorized writing device.

2.5.2.2 Confidentiality

1) Air interface confidentiality
Written data and writing mechanism confidentiality
2) UIM/MS-to-writing device confidentiality
Written data and writing mechanism confidentiality
3) UIM-to-UIM administrator confidentiality
Written data and writing mechanism confidentiality on the channel between UIM and UIM administrator (End to End).
4) Stored data confidentiality
Function of encrypting written data and storing in record media. Data disclosure and data forgery prevention by procedures except formal interface.

2.5.3 UIM/MS Data Writing Design Principle

Requirements for guaranteeing UIM/MS data writing security are:
- Strength for writing (making the mechanism, algorithm and key generation algorithm complex)
- Limiting the confidentiality scope (to be disclosed or standardized)
- UIM administrator proprietary procedure

Considering the above conditions, UIM/MS data writing design guideline shall be as follows:

2.5.3.1 Removable UIM

1) Data writing by writing device
Each functionality must be at the discretion of UIM administrator.
2) Data writing by OTA
The air interface confidentiality mechanism and algorithm should be specified. Other functionality must be at the discretion of UIM administrator.
The functional requirement of the mechanism and algorithm is the same as that of confidentiality for call control.

2.5.3.2 Non-Removable UIM

1) Data writing by writing device
It is required to standardize each functionality in order to realize a common procedure for data writing. In IMT-2000 system, it is required to disclose technical information to equipment manufactures (for MS/writing device) on global basis. Therefore a technology and its operational method to guarantee security on these conditions must be studied. If the above technology and the operational method are hard to realize, it is required to consider a UIM administrator proprietary procedure for data writing to guarantee security.
2) Data writing by OTA
In addition to the similar questions in data writing by writing device, a technology and its operational method must be studied to prevent lower security level due to the radio interface use.

Necessity of Future Study

3.1 Security Management Area

- Management of 3G Mobile System specific security mechanisms and algorithms
  Update and control of the security mechanism and algorithm is for further study.
- Key management
  The authentication key generation algorithm and encryption key generation algorithm are specified.
- Encryption management
  The user data confidentiality and the signalling information confidentiality are specified. The user location confidentiality is not necessary for study if it is possible using the air interface confidentiality and a temporary ID.
- Authentication management
  The authentication algorithm is specified.
- Access control management
  The access control for subscription and service profile data is not subject to study.
- Service barring list management
  Not subject to study. It is regarded as access control for supplementary services.
- Security audit management
  For further study (It shall be studied when it is clearly defined.)
- Management of subscriber related credential information
  For further study (It shall be studied when it is clearly defined.)
- Information exchange regarding security management
  For further study (It shall be studied when it is clearly defined.)

3.2 Security and Private Services

- Transaction Security
  It is specified this time.
- End-to-end encryption
  Not subject to study if end-to-end means service provider to user.
  For further study if end-to-end means terminal to terminal.
- Password call acceptance
  Not subject to study.
- Subscriber PIN access & intercept
  Not subject to study.
- Procedure for the Change of Keyword (FWA)
  For further study (it shall be studied when it is clearly defined.)
- Signaling information element confidentiality
  It is specified this time.

4. Work Plan in Stage 2

In Stage 2, concrete security algorithms will be studied based on this design principle.
The study members mainly include security experts. However some mobile radio experts are required to join.
As the specification must be ready by April 1999, it is more realistic to start with existing mechanisms and to select algorithms from the existing ones instead of creating new ones for IMT-2000, because of the time constraint. However, taking into account the work progress and the status of technological development, the above policy is not necessarily mandatory.
Also, in terms of the data writing mechanism/algorithm for non-removable UIM in chapter

2.5.3 “UIM/MS data writing design guideline”, it is difficult to quickly select a technology and its operational method in which security against cryptanalysis is possible in the case that the technical information of UIM data writing is disclosed to equipment manufacturers on global basis. Therefore, it is desirable to study all security functions, excluding OTA, based on removable UIM in Phase 1.

However, taking into account that the both of removable and non-removable UIMs are under study for the ANSI evolution since compatibility with the 2nd generation is strongly required, it is required to specify standards for the subscriber data writing. Measures to realize it using OTASP (Over-the-Air Service Provisioning), ROM writer and so forth, are seen. It is required to develop and standardize a technology and its operational method by taking much care of preserving security when the writing technology is disclosed to equipment manufacturers. Since the content of the subscribe data writing standard is limited and the subscriber data writing standard includes confidential matters even in the process of documentation, it shall be documented in a separate volume. It shall be able to disclose the main volume so that range of disclosure can be limited because of the same reason above, by separating it into ANSI evolution and GSM evolution parts.

As a summary, Table A8-4 shows functions to be standardized for the ANSI and GSM evolutions.

Table A8-4 Functions to be standardized in Phase 1 for the ANSI and GSM evolutions

Item no.	Item		Mechanism		Algorithm		Key generation algorithm	
			ANSI	GSM	ANSI	GSM	ANSI	GSM
1	User Identity Authentication		O	O	O	O	O	X
2	Re-authentication of Users		O	O	O	X	O	X
3	Network Operator / Service Provider Authentication		O	X	O	X	O	X
4	User Data Confidentiality		O	O	O	O	O	X
5	Signalling Information Confidentiality		O	O	O	O	O	X
6	User Identity Confidentiality (temporary ID)		O	O	X	X	X	X
7	User Location Confidentiality		O	O	X	X	X	X
8	Access Control for Subscription and Service Profile Data		X	X	X	X	X	X
9	Version Control of Security Data and Mechanisms		O	O	X	X	X	X
10	Writing subscriber data to UIM	Removable	X	X	X	X	X	X
		Non-Removable	O(note)	-	O(note)	-	O(note)	-
11	Emergency Call		O	O	O	O	O	O

(Note): This item requires considerations for confidentiality.