INTERNATIONAL TELECOMMUNICATION UNION

ITU-T X.1121

(04/2004)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

Telecommunication security

Framework of security technologies for mobile end-to-end data communications

ITU-T Recommendation X.1121

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	**X.1000–**

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation X.1121

Framework of security technologies for mobile end-to-end data communications

Summary

This Recommendation describes the security threats to mobile end-to-end data communications and the security requirements from the point of view of the mobile users and application service providers (ASP). In addition, this Recommendation shows where the security technologies which realize certain security function appear in the models of mobile end-to-end data communications.

Source

ITU-T Recommendation X.1121 was approved on 29 April 2004 by ITU-T Study Group 17 (2001-2004) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation X.1121

Framework of security technologies for mobile end-to-end data communications

1 Scope

This Recommendation provides security requirements, from the point of view of the mobile user and the application service provider in the upper layer of the OSI Reference Model, for mobile end-to-end data communications between a mobile terminal in a mobile network and an application server in an open network.

This Recommendation provides a framework of security technologies for mobile end-to-end data communications.

This Recommendation does not provide the details of mobile network components except for wireless network access to a mobile terminal when connected to an open network.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation

– ITU-T Recommendation Q.1701 (1999), *Framework for IMT-2000 networks*.

– ITU-T Recommendation Q.1711 (1999), *Network functional model for IMT-2000*.

– ITU-T Recommendation Q.1761 (2004), *Principles and requirements for convergence of fixed and existing IMT-2000 systems*.

– ITU-T Recommendation X.800 (1991), *Security Architecture for Open Systems Interconnection for CCITT applications*.

– ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.

– ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

3 Definitions

3.1 OSI Reference Model security architecture definitions

The following terms are defined in ITU-T Rec. X.800:

a) access control;

b) authentication;

c) authentication information;

d) authentication exchange;

e) authorization;

f) availability;

g) confidentiality;

h) cryptography;

i) data integrity;

j) data origin authentication;

k) encipherment;

l) integrity;

m) key;

n) key exchange;

o) key management;

p) non-repudiation;

q) notarization;

r) password;

s) privacy.

3.2 Additional definitions

This Recommendation defines the following terms:

3.2.1 anonymity: Ability to allow anonymous access to services, which avoid tracking of user's personal information and user behaviour such as user location, frequency of a service usage, and so on.

3.2.2 shoulder surfing: A security threat which collects information in busy places by watching keystroke, reading mobile terminal's screen, or listening to sound from a mobile terminal.

3.2.3 mobile terminal: An entity that has wireless network access function and connects a mobile network for data communication with application servers or other mobile terminals.

3.2.4 mobile network: A network that provides wireless network access points to mobile terminals.

3.2.5 mobile user: An entity (person) that uses and operates the mobile terminal for receiving various services from application service providers.

3.2.6 application service: A service like mobile banking, mobile commerce, and so on.

3.2.7 application server: An entity that connects to an open network for data communication with mobile terminals.

3.2.8 Application Service Provider (ASP): An entity (person or group) which provides application service(s) to mobile users through an application server.

3.2.9 mobile security gateway: An entity which relays data communication between a mobile terminal and an application server, changes security parameters or communication protocol from a mobile network to an open network, or vice versa, and can perform security policy management functions for mobile end-to-end data communication.

3.2.10 security policy management: A function to manage or negotiate a set of rules to provide classified security services which can be implemented on the mobile security gateway or other server.

4 Abbreviations

This Recommendation uses the following abbreviations:

ASP	Application Service Provider
DoS	Denial of Service
IMT-2000	International Mobile Telecommunications-2000
LAN	Local Area Network
OSI	Open Systems Interconnection
PC	Personal Computer
PDA	Personal Data Assistant
PIN	Personal Identification Number

5 Overview

Mobile terminals with data communication capabilities (like IMT-2000 mobile phone, laptop PC or a PDA with a radio-card) have been widely distributed and various application services (e.g., mobile commerce) for mobile terminals are provided through the mobile network. In the e-commerce application, security is necessary and indispensable.

There are many areas under investigation from a mobile operator's point of view (e.g., security architecture on IMT-2000 mobile telephone network). However, it is also important to investigate from the mobile user's point of view and the ASP's point of view.

When investigating security in a mobile communication from the mobile user's point of view or ASP's point of view, security for mobile end-to-end data communication between a mobile terminal and an application server is one of the most important aspects.

In addition, for the mobile system that connects a mobile network to an open network, security investigation in the upper layers (applications, presentation and session layers) of the OSI Reference Model is needed because there are various implementations of mobile network (for example, IMT-2000 mobile phone network, wireless LAN, Bluetooth) or open network.

This Recommendation describes the security threats to mobile end-to-end data communications and the security requirements from the point of view of the mobile user and the ASP. In addition, this Recommendation shows where the security technologies which realize certain security function appear in the models of mobile end-to-end data communications.

6 Models of mobile end-to-end data communications

Before describing secure mobile technologies, models of mobile end-to-end data communication should be defined. Models of mobile end-to-end data communication clarify the relationship between entities in models and the points to which the secure mobile technologies should be adapted.

6.1 General model of mobile end-to-end data communication between the mobile user and the ASP

A general model of mobile end-to-end data communication between a mobile user and an ASP is shown in Figure 1.

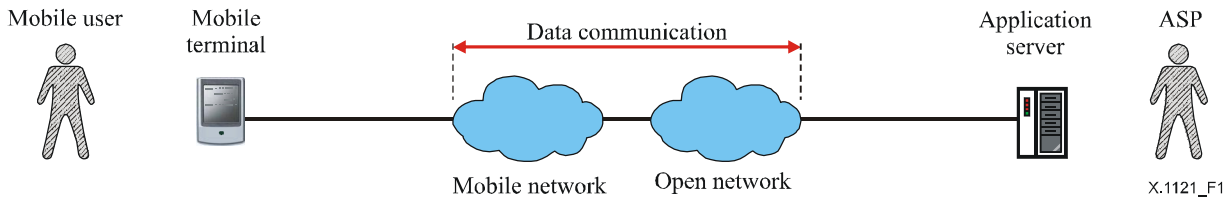

Figure 1/X.1121 – General model of mobile end-to-end data communication between a mobile user and an ASP

There are six entities in this model: mobile user, mobile terminal, mobile network, open network, application server and ASP.

And there are five relationships in this model, between: mobile user and mobile terminal, mobile terminal and mobile network, mobile network and open network, open network and application server, and mobile terminal and application server.

6.2 Gateway model of mobile end-to-end data communication between the mobile user and the ASP

Another model (Gateway model) of mobile end-to-end data communication between a mobile user and an ASP is shown in Figure 2.

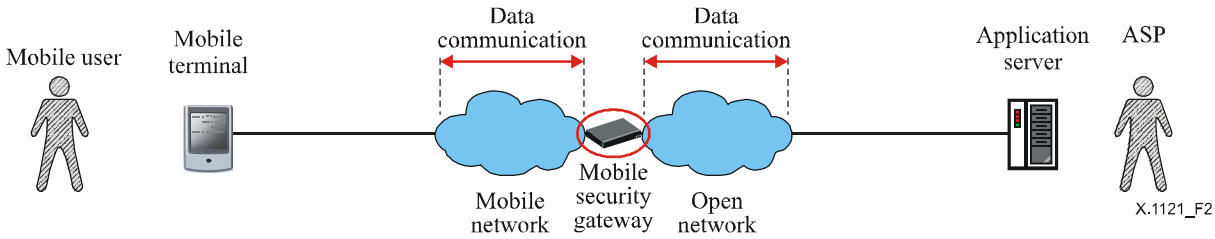

Figure 2/X.1121 – Gateway model of mobile end-to-end data communication between a mobile user and an ASP

There are seven entities in this model: mobile user, mobile terminal, mobile network, open network, application server, ASP and mobile security gateway.

And there are seven relationships in this model, between: mobile user and mobile terminal, mobile terminal and mobile network, mobile network and mobile security gateway, mobile security gateway and open network, open network and application server, mobile terminal and mobile security gateway, and mobile security gateway and application server.

7 Characteristics of mobile end-to-end data communication

Mobile end-to-end data communication has various characteristics compared to general end-to-end data communication in an open network. These characteristics are listed below:

Mobile communication is based on wireless communication

Because mobile end-to-end data communication is based on wireless communication, it is more unstable than a wired end-to-end data communication in an open network. In addition, because a mobile user can move around during mobile end-to-end data communication, it adds further instability.

Wireless communication could be based on broadcast communication between a mobile terminal and a mobile network.

Mobile terminals are small terminals in general

In general, mobile terminals that are used for mobile end-to-end data communication are smaller than existing typical terminals (e.g., desktop PC) that are used for end-to-end data communication in an open network. The consequences are:

– difficulty of data input or output;

  It is difficult to enter data through keyboard or keypad and to see many data through its screen because of limited space of screen (especially, in the case of a small-sized hand-held terminal);

– lower processing performance than desktop PC;

– limitation on corresponding application capacity (memory size, supply of power, etc.).

Mobile terminals are carried around by mobile users

8 Security threats to the mobile environment

There are two types of security threats. One relates to general security threats that might exist in any open network. The other relates to mobile-oriented security threats that might exist due to the characteristics of mobile communications.

8.1 General security threats

As a subset of end-to-end data communications, mobile end-to-end data communications are also vulnerable to general security threats that are present in the open networks.

8.1.1 Eavesdropping

The most widely identified problem in open networks is the susceptibility to eavesdropping by anonymous attacks. Anonymous attackers can actively intercept transmitted data, causing a leakage of data.

8.1.2 Communication jamming

This takes place when an intentional or unintentional interference overpowers the sender or receiver of a communication link, thereby effectively rendering the communication link useless. This can result in a DoS attack.

8.1.3 Injection and modification of data

This occurs when an unauthorized entity inserts, changes or deletes information transmitted between a mobile terminal and an application server. The unauthorized entity could be a person, a program, or a computer. These attacks occur when an attacker adds data to an existing connection with the objective of hijacking the connection or maliciously sending data. This can result in a DoS attack or man-in-the-middle attack.

8.1.4 Interruption

This type of attack results in the destruction of a component of a mobile terminal or a network element, examples being destruction of a piece of hardware, such as a hard disk; the cutting of a communication line; or the disabling of the file management system in a mobile terminal or a network element in the mobile network infrastructure.

8.1.5 Unauthorized access

Access control is the ability to limit and control the access to an application server via a communication link. This threat occurs when an illegal entity gains access to an application server by masquerading as a real mobile user. The entity trying to gain an unauthorized access must be identified, or authenticated.

8.1.6 Repudiation

This attack occurs when a sender or receiver denies the fact of having transmitted or received a message, respectively.

8.2 Mobile-oriented security threats

There are mobile-oriented security threats resulting from characteristics of mobile communications, especially in the case of wireless communication and broadcast communication between a mobile terminal and a mobile network. The most widely identified problem in a wireless network is that it is susceptible to anonymous attackers.

Mobile-oriented security threats are listed below.

8.2.1 Eavesdropping

In mobile communications, this can be carried out more easily by actively intercepting radio signals and decoding the data being transmitted, causing a leakage of data.

8.2.2 Communication jamming

In mobile communications, this can also be carried out more easily between a mobile terminal and a mobile network. There are two types of attacks: jamming against a mobile terminal and jamming against a network element. The former allows a rogue mobile terminal to impersonate the legal mobile terminal. The latter impersonates the legitimate network element interfacing with the mobile terminal through the wireless interface.

8.2.3 Shoulder surfing

This occurs when an attacker collects information in busy places by watching keystroke, reading a mobile terminal's screen, or listening to sound from a mobile terminal. This results in leakage of information.

8.2.4 Lost mobile terminal

This security threat may occur as the mobile terminal is carried around by the mobile user. This can result in the loss or destruction of information stored in the mobile terminal.

8.2.5 Stolen mobile terminal

This threat may also occur as the mobile terminal is carried around by the mobile user. This can cause leakage of information stored in the mobile terminal, data deletion resulting from unauthorized access of the stolen mobile terminal in addition to the loss of information stored in the mobile terminal.

8.2.6 Unprepared communication shutdown

This is a security threat caused by unstable communication or the limitation of power supply. This can result in data deletion.

8.2.7 Misreading

This is a security threat caused by a small display of mobile terminals. This can result in data deletion by masquerading of ASP.

8.2.8 Input error

This is a security threat caused by the difficulty of inputting data via a small keyboard or the keypad of a mobile terminal. This can cause the failure of user authentication.

8.3 Relationship of security threats to end-to-end communication models

These security threats appear in particular places of models. The relationship of security threats and functional entities in models is shown in Tables 1 and 2.

These tables show that there are the same security threats in an application server and a mobile security gateway. These tables also show that there are similar security threats in the relation between: mobile terminal and application server; mobile terminal and mobile security gateway; application server and mobile security gateway.

Table 1/X.1121 – Relationship of general security threats to models

Threats / Entities, Relations	Eavesdropping	Communication jamming	Injection/ Modification	Interruption	Unauthorized access	Repudiation
Mobile terminal				X	X	
Application server		X		X	X	
Relation between mobile user and mobile terminal						
Relation between mobile terminal and application server	X	X	X	X		X
Mobile security gateway				X	X	
Relation between mobile terminal and mobile security gateway	X	X	X	X		X
Relation between application server and mobile security gateway	X	X	X	X		X

Table 2/X.1121 – Relationship of mobile-oriented security threats to models

Threats / Entities, Relations	Eavesdropping	Communication jamming	Shoulder surfing	Lost/Stolen terminal	Unprepared shutdown	Misreading/ Input error
Mobile terminal		X		X		
Application server						
Relation between mobile user and mobile terminal			X			X
Relation between mobile terminal and application server	X	X			X	
Mobile security gateway		X				
Relation between mobile terminal and mobile security gateway	X	X			X	
Relation between application server and mobile security gateway	X	X			X	

9 Security requirements for mobile end-to-end data communications

There are two types of security requirements for mobile end-to-end data communications. One relates to the mobile user's point of view. The other relates to the ASP's point of view.

9.1 Security requirements from the mobile user's point of view

There are many different user expectations and needs when it comes to applications. What is common to most mobile users is their simple expectation that the application works and is user-friendly. Most people expect the applications and service providers to handle their personal data in a secure and privacy-respecting way. In order to achieve this expectation, the mobile user sets conditions in the following information security areas:

– identity management;
– data confidentiality;
– data integrity;
– authentication;
– access control;
– non-repudiation;
– anonymity;
– privacy;
– usability;
– availability.

9.1.1 Identity management

Identity management typically relates to the protection of user identity information. Therefore, identity management is a very important aspect of user privacy. Pseudonyms can be used during communication. The mobile user's identity management requirement is to generate (or request to generate), maintain, delete (or request to delete), and apply the keys in accordance with mobile user's security policy.

9.1.2 Data confidentiality

The mobile user's data confidentiality requirements consist of the following:

Communication data confidentiality between a mobile terminal and an application server

This provides confidentiality of all or sensitive data transmitted between the mobile terminal and an application server.

Stored data confidentiality on a mobile terminal

This provides confidentiality of all or sensitive data stored in a mobile terminal.

Stored data confidentiality on an application server

This provides confidentiality of all or sensitive data in an application server that are associated with the mobile user.

In the "Gateway model", the mobile user's data confidentiality requirements also cover:

Communication data confidentiality between a mobile terminal and a mobile security gateway

This provides confidentiality of all or sensitive data transmitted between the mobile terminal and a mobile security gateway.

Communication data confidentiality between an application server and a mobile security gateway

This provides confidentiality of all or sensitive data transmitted between an application server and a mobile security gateway.

Stored data confidentiality on a mobile security gateway

This provides confidentiality of all or sensitive data stored in a mobile security gateway.

9.1.3 Data integrity

The mobile user's data integrity requirements consist of the following:

Communication data integrity between a mobile terminal and an application server

This provides integrity of all communication data between the mobile terminal and an application server.

Stored data integrity on a mobile terminal

This provides integrity of all data stored in the mobile terminal.

Stored data integrity on an application server

This provides integrity of all data stored in an application server that are associated with the mobile user (for example, mobile user's personal information).

In the "Gateway model", the mobile user's data integrity requirements also cover:

Communication data integrity between a mobile terminal and a mobile security gateway

This provides integrity of all data transmitted between the mobile terminal and a mobile security gateway.

Communication data integrity between an application server and a mobile security gateway

This provides integrity of all data transmitted between an application server and a mobile security gateway.

Stored data integrity on a mobile security gateway

This provides integrity of all data stored in a mobile security gateway that is associated with the mobile user.

9.1.4 Authentication

There are two types of authentication: entity and message authentication. The entity authentication is for one entity to prove its identity to a corresponding entity. The message authentication is to prove the origin of data or receipt of data. The mobile user's authentication requirements consist of the following:

ASP authentication

This is a type of entity authentication used to confirm the identity of an ASP in order to reassure that the ASP is not attempting a masquerade or unauthorized replay of a previous connection.

Mobile user authentication

This is a type of entity authentication employed to prove the identity of the user of a mobile terminal by implementing various user authentication schemes such as finger printing, password, or PIN in order to provide protection against unauthorized access from a lost or stolen mobile terminal.

Received data authentication

This is a type of message authentication used to corroborate the source of communication data. This does not request the provision of protection against duplication or modification of data.

9.1.5 Access control

The mobile user's access control requirements consist of the following:

Access control on a mobile terminal

This provides protection against unauthorized access to or unauthorized use of a mobile terminal.

The access control will be in accordance with the mobile user's security policies.

Access control on an application server

This provides protection against unauthorized access of an application server to the data sent by a mobile user such as the mobile user's personal information.

The access control will be in accordance with the mobile user's security policies.

In the "Gateway model", the mobile user's access control requirements also cover:

Access control on a mobile security gateway

This provides protection on a mobile security gateway against unauthorized access to the data sent by a mobile user such as the mobile user's personal information.

The access control will be in accordance with the mobile user's security policies.

9.1.6 Non-repudiation

This exists as one or both of the two variants below:

Non-repudiation with proof of origin

This is used to prove that the origin of received data is a particular ASP. This is required to protect against any attempt by the ASP to falsely deny sending the data.

Non-repudiation with proof of delivery

This is used to provide the proof of delivery of data to an ASP. This is required to protect against any subsequent attempt by the ASP to falsely deny receiving the data.

Non-repudiation requirements are linked to the following requirements: communication data confidentiality between a mobile terminal and an application server; communication data integrity between a mobile terminal and an application server; stored data integrity on a mobile terminal; mobile user authentication and access control on a mobile terminal.

The "Gateway model" is linked to the following requirements: communication data confidentiality between a mobile terminal and a mobile security gateway; communication data confidentiality between a mobile security gateway and an application server; communication data integrity between a mobile terminal and a mobile security gateway; communication data integrity between a mobile security gateway and an application server; stored data integrity on a mobile security gateway.

9.1.7 Anonymity

This enables the sending of a message so that the ASP cannot identify the mobile user (and mobile terminal).

9.1.8 Privacy

This is used to avoid leakage of information and to prevent an unauthorized person from obtaining the information.

Privacy requirements are linked to the following requirements: communication data confidentiality between a mobile terminal and an application server; stored data confidentiality on a mobile terminal, stored data confidentiality on an application server; access control on a mobile terminal and access control on an application server.

The "Gateway model" is linked to the following requirements: communication data confidentiality between a mobile terminal and a mobile security gateway, communication data confidentiality between a mobile security gateway and an application server; stored data confidentiality on mobile security gateway and access control on a mobile security gateway.

9.1.9 Usability

This provides easy use of an application and avoids misreading or errored input.

9.1.10 Availability

This provides the mobile user with the ability to receive an application service from anywhere and at anytime.

9.2 Security requirements for ASP's point of view

Businesses which offer their services to mobile users have to protect their systems against fraud. Because of the specificities of mobile equipment, subscriber authentication and payment mechanisms should be managed carefully. Furthermore, if a service is delivered to the mobile users, non-repudiation and traceability of the service cannot be avoided. Therefore, the ASP has requirements in the following areas:

– data confidentiality;
– data integrity;
– authentication;
– access control;
– non-repudiation;
– availability.

9.2.1 Data confidentiality

The ASP's data confidentiality requirements consist of the following:

Communication data confidentiality between a mobile terminal and the application server

This provides confidentiality of all or sensitive data transmitted between a mobile terminal and the application server.

Stored data confidentiality on a mobile terminal

This provides confidentiality of all or sensitive data or contents that are sent by the ASP and stored in a mobile terminal.

Stored data confidentiality on an application server

This provides confidentiality of all data stored in the application server.

In the "Gateway model", the ASP's data confidentiality requirements also cover:

Communication data confidentiality between a mobile terminal and a mobile security gateway

This provides confidentiality of all or sensitive data transmitted between a mobile terminal and a mobile security gateway.

Communication data confidentiality between an application server and a mobile security gateway

This provides confidentiality of all or sensitive data transmitted between the application server and a mobile security gateway.

Stored data confidentiality on a mobile security gateway

This provides confidentiality of all or sensitive data (or contents) that are sent by the ASP and stored in a mobile security gateway.

9.2.2 Data integrity

The ASP's data integrity requirements consist of the following:

Communication data integrity between a mobile terminal and an application server

This provides integrity of all communication data between a mobile terminal and the application server.

Stored data integrity on a mobile terminal

This provides integrity of all data or contents that are sent by the ASP and stored in a mobile terminal.

Stored data integrity on an application server

This provides integrity of all data stored in the application server.

In the "Gateway model", the ASP's data integrity requirements also cover:

Communication data integrity between a mobile terminal and a mobile security gateway

This provides integrity of all (or part of) data transmitted between a mobile terminal and a mobile security gateway.

Communication data integrity between an application server and a mobile security gateway

This provides integrity of all data transmitted between the application server and a mobile security gateway.

Stored data integrity on a mobile security gateway

This provides integrity of all data or contents that are sent by the ASP and stored in a mobile security gateway.

9.2.3 Authentication

The ASP's authentication requirements also consist of entity authentication (mobile user and mobile terminal) and message authentication (received data).

Mobile user authentication

This is a type of entity authentication used to confirm the identity of a mobile user in order to reassure that a mobile user is not attempting a masquerade or unauthorized replay of a previous connection.

Mobile terminal authentication

This is a type of entity authentication used to confirm the identity of a mobile terminal to ensure that a mobile terminal has the functionality necessary to access an application service.

Received data authentication

This is a type of message authentication used to corroborate the source of communication data. This does not request the provision of protection against duplication or modification of data.

9.2.4 Access control

The ASP's access control requirements consist of access control on the application server and access control on the mobile terminal.

Access control on an application server

This provides protection against unauthorized access to or unauthorized use of an application server.

The access control will be in accordance with the ASP's security policies.

Access control on a mobile terminal

This provides protection against unauthorized access to data or contents sent by the ASP on a mobile terminal.

The access control will be in accordance with the ASP's security policies.

In the "Gateway model", the ASP's access control requirements also cover:

Access control on a mobile security gateway

This provides protection against unauthorized access to data or contents sent by the ASP on a mobile security gateway.

The access control will be in accordance with the ASP's security policies.

9.2.5 Non-repudiation

This exists as one or both of the two variants below:

Non-repudiation with proof of origin

This is used to prove that the origin of received data is a particular mobile user. This is also required to protect against any attempt by the mobile user to falsely deny sending the data or its contents.

Non-repudiation with proof of delivery

This is used to provide the proof of delivery of data to a mobile user. This is also required to protect against any subsequent attempt by the mobile user to falsely deny receiving the data or its contents.

The ASP's non-repudiation requirements are linked to the following: communication data confidentiality between a mobile terminal and an application server; communication data integrity between a mobile terminal and an application server; stored data integrity on a mobile terminal; mobile user authentication and access control on a mobile terminal.

The "Gateway model" is linked to the following requirements: communication data confidentiality between a mobile terminal and a mobile security gateway; communication data confidentiality between a mobile security gateway and an application server; communication data integrity between a mobile terminal and a mobile security gateway; communication data integrity between a mobile security gateway and an application server; stored data integrity on a mobile security gateway.

9.2.6 Availability

This provides the authorized mobile user with the ability to receive an application service from anywhere and at anytime.

9.3 Relationship between security requirements and security threats

Each security requirement is a countermeasure against certain security threats. The relationship between security requirements and security threats is shown in Tables 3 and 4.

Table 3/X.1121 – Relationship between security requirements and general security threats

Requirements \ Threats	Eavesdropping	Communication jamming	Injection/ Modification	Interruption	Unauthorized access	Repudiation
Identity management	X				X	X
Communication data confidentiality	X					
Stored data confidentiality					X	
Communication data integrity			X			
Stored data integrity					X	
Entity authentication			X		X	X
Message authentication			X			
Access control			X		X	
Non-repudiation						X
Anonymity					X	
Privacy	X				X	
Usability						
Availability		X		X		

Table 4/X.1121 – Relationship between security requirements and mobile-oriented security threats

Requirements \ Threats	Eavesdropping	Communication jamming	Shoulder surfing	Lost/Stolen terminal	Unprepared shutdown	Misreading/ Input error
Identity management	X					
Communication data confidentiality	X					
Stored data confidentiality				X		
Communication data integrity						
Stored data integrity				X		
Entity authentication				X		
Message authentication						

Access control				X		
Non-repudiation						
Anonymity				X		
Privacy	X		X	X		
Usability						X
Availability		X			X	

10 Security functions for satisfying mobile security requirements

To achieve security requirements for mobile end-to-end data communications, there are several security functions that may be used as follows:

– encipherment;
– key exchange;
– digital signature;
– access control;
– data integrity;
– authentication exchange;
– notarization.

Encipherment

The encipherment function can provide confidentiality of either communication data or stored data.

Encipherment algorithms may be reversible or irreversible. There are two general classifications of reversible encipherment algorithm:

a) Symmetric (i.e., secret key) encipherment, in which knowledge of the encipherment key implies knowledge of the decipherment key and vice versa; and

b) Asymmetric (e.g., public key) encipherment, in which knowledge of the encipherment key does not imply knowledge of the decipherment key, or vice versa. The two keys of such a system are sometimes referred to as the "public key" and the "private key".

Irreversible encipherment algorithms may or may not use a key. When they use a key, this key may be public or secret.

Because of the low processing capability or small memory size of mobile terminals, there are some difficulties in implementing existing encipherment functions, especially asymmetric algorithm, used in existing open networks. In the case of continuing the use of existing encipherment functions on a server in open networks, the gateway model is often used.

Key exchange

The key exchange function allows for key sharing in encipherment implementations, especially that of the symmetric encipherment algorithm.

Digital signature

The digital signature function defines two processes:

a) signing a data; and

b) verifying a signed data.

The first process uses information that is private (i.e., unique and confidential) to the signatory. The second process uses procedures and information which are publicly available but from which the signatory's private information cannot be deduced.

The signing process involves either an encipherment of the data or the production of a cryptographic check value of the data, using the signatory's private information as a private key.

The verification process involves the use of public procedures and information to determine whether the signature was produced correctly with the signatory's private information.

The essential characteristic of the signature function is that the signature can only be produced using the signatory's private information. Thus, when the signature is verified, it can subsequently be proven to a third party (e.g., a judge or arbitrator) at any time that only the unique holder of the private information could have produced the signature.

As for encipherment function, due to the low processing performance or small memory size of mobile terminals, there are some difficulties in implementing the existing digital signature functions used in existing open networks.

Access control

The access control function may use the authenticated identity of an entity or information about the entity (such as membership in a known set of entities) or capabilities of the entity, in order to determine and enforce the access rights of the entity. If the entity attempts to use an unauthorized resource, or an authorized resource with an improper type of access, then the access control function will reject the attempt and may additionally report the incident for the purposes of generating an alarm and/or recording it as part of a security audit trail.

The access control function may be based on the use of the following items:

a) access control information bases, where the access rights of peer entities are maintained in a database;

b) authentication information such as passwords, possession and subsequent presentation of which is evidence of the accessing entity's authorization;

c) capabilities, possession and subsequent presentation of which is evidence of the right to access the entity or resource defined by the capability;

d) security labels, which when associated with an entity may be used to grant or deny access, usually according to a security policy;

e) time of attempted access;

f) route of attempted access;

g) duration of access; and

h) physical location of attempted access.

The access control function may be applied at either peer entities of a communication association and/or at a mobile security gateway.

Access control involved at the origin entity or mobile security gateway is used to determine whether the sender is authorized to communicate with the recipient and/or to use the required communication resources.

Data integrity

Two aspects of data integrity are considered: the integrity of a single data unit or field and the integrity of a stream of data units or fields. In general, different technologies are used to provide these two types of integrity function, although provision of the second without the first is not practical.

Determining the integrity of a single data unit involves two processes: one at the sending entity and one at the receiving entity. The sending entity appends to data a quantity that is a function of the data itself. This quantity may be supplementary information such as a block check code or a cryptographic check value and it may be enciphered. The receiving entity generates a corresponding

quantity and compares its result with the received quantity to determine whether the data have been modified in transit. This process alone will not protect against the replay of a single data unit.

Protecting the integrity of a sequence of data units (i.e., protecting against disordering, losing, replaying and inserting or modifying data) requires the addition of some form of explicit ordering such as sequence numbering, time stamping, or cryptographic chaining.

Authentication exchange

Some security technologies that may be applied to authentication exchanges are:

a) use of authentication information, such as passwords supplied by a sending entity and checked by the receiving entity;

b) cryptographic technologies; and

c) use of characteristics and/or possessions of the entity.

The authentication exchange function may be incorporated in order to provide peer entity authentication. If the function does not succeed in authenticating the entity, this will result in rejection or termination of the connection and may cause an entry in the security audit trail and/or a report to a security management centre.

When cryptographic techniques are used, they may be combined with "handshaking" protocols to protect against replay (i.e., to ensure liveness).

The choices of security technologies, which realize authentication exchange, will depend upon the circumstances in which they need to be used with:

a) time stamping and synchronized clocks;

b) two- and three-way handshakes (for unilateral and mutual authentication respectively); and

c) non-repudiation functions achieved by digital signature and/or notarization mechanisms.

Notarization

Properties of the data communicated between two or more entities, such as its integrity, origin, time and destination, can be assured by the provision of a notarization function. The assurance is provided by a third party notary, which is the communicating entities trust, and which holds the necessary information to provide the required assurance in a verifiable manner. Each instance of communication may use digital signature, encipherment, and integrity functions as appropriate to the service being provided by the notary. When such a notarization function is invoked, the data are communicated between the communicating entities via the protected instances of communication and the notary.

These security functions are used to satisfy some of the security requirements. Which functions satisfy which security requirements are shown in Table 5.

Table 5/X.1121 – Illustration of relationship between security requirements and functions

Requirements \ Functions	Encipherment	Key exchange	Digital signature	Access control	Data integrity	Authentication exchange	Notarization
Identity management	X	X	X			X	
Communication data confidentiality	X	X		X		X	
Stored data confidentiality	X			X			
Communication data integrity	X	X	X	X	X	X	
Stored data integrity	X		X	X	X		
Entity authentication	X		X			X	
Message authentication	X	X	X		X	X	
Access control				X		X	
Non-repudiation			X			X	X
Anonymity	X						
Usability				X			
Privacy	X			X		X	
Availability				X		X	

11 Security technologies for mobile end-to-end data communication

To realize the security functions as described in clause 10, various security technologies for mobile end-to-end data communication (i.e., secure mobile technologies) are used. These secure mobile technologies are categorized by security functions realized by the security technology and where the security technology applies. Because a security technology applies to an entity or a relation between entities in models of mobile end-to-end data communication, the places at which the security technology is applied denote entities or relations between entities. Tables 1 and 2 show where security threats appear in models of mobile end-to-end data communication. Tables 3 and 4 show which security requirements are developed as countermeasures to particular security threats, and Table 5 shows the security functions which meet the security requirements. Therefore, the relationship between security functions and places to apply these security functions in models can be shown in Table 6. In other words, Table 6 shows where mobile security technologies, which realize certain security functions, are applied to in models.

Particular mobile security technology may realize only a part of the security functions or be applied to a particular place. For example, the elliptic curve cryptographic algorithm can be used to realize a Key Exchange function in the relation between the user and a mobile terminal. Biometrics authentication technology can be used to realize Authentication Exchange function in the relation between the user and a mobile terminal. PKI technology can be used to realize all security functions in the relation between a mobile terminal and a server, the relation between a mobile terminal and a mobile security gateway, and the relation between a server and a mobile security gateway.

Table 6/X.1121 – Relationship between secure mobile technologies and models

Functions realized by technologies \ Places to which technologies apply	Mobile terminal	Application server/ Mobile security gateway	Relation between mobile user and mobile terminal	Relation between mobile terminal and application server or other relations
Encipherment	X	X	X	X
Key Exchange				X
Digital Signature	X	X		X
Access Control	X	X	X	X
Data Integrity	X	X		X
Authentication Exchange	X	X	X	X
Notarization				X

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signaling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks and open system communications**
Series Y	Global information infrastructure, Internet protocol aspects and Next Generation Networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2004