3GPP TSG SA WG3 Security - S3#37 S3-050003

21 - 25 February 2004, Sophia Antipolis, France

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2005-2008

COM 17 – LS 05 – E

English only

Original: English

Question(s):	9/17

LIAISON STATEMENT

Source:	Q.9/17 Rapporteur Group (Tokyo, 15-17 November 2004)
Title:	Liaison on General Security Policy for Secure Mobile End-to-End Data Communication

LIAISON STATEMENT

To:	3GPP, 3GPP2, SG 19	
Approval:	Agreed at Q.4-9/17 Joint Rapporteurs meeting	
For:	Information/Action	
Deadline:	None	
Contact:	Dr. Heung Youl Youm Soonchunhyang Univ. Korea	Tel: +82 41 530 1328 Fax: +82 41 530 1494 Email: hyyoum@sch.ac.kr

Please don’t change the structure of this table, just insert the necessary information.

With this liaison we would like to inform you that Q.9/17 starts to study “General Security Policy for Secure Mobile End-to-end Data Communication”.

For the 2005-2008 study period of ITU-T, we will continue to study general security policy in mobile network that can provide additional security protection as value added service. We envision that we could use the results to pursue flexible security protection for mobile network that not only benefits end users but also benefits service providers.

For your information we attach some material that provides some further information about general security policy for end-to-end data communication.

We are interested to receive your feedback and are looking forward to collaborating with you on these matters.

Attachment: Draft X.msec-3 “General security policy for secure mobile end-to-end data communication”.

Attention: Some or all of the material attached to this liaison statement may be subject to ITU copyright. In such a case this will be indicated in the individual document.
Such a copyright does not prevent the use of the material for its intended purpose, but it prevents the reproduction of all or part of it in a publication without the authorization of ITU.

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU

ATTACHMENT

Draft Rec. X.msec-3

General security policy for secure mobile end-to-end data communication

Summary

This baseline document of x.msec-3 describes general security policy for secure mobile end-to-end data communication. The investigation of general security policy is important for both service providers and users. The service providers can use the general security policy to overcome limits of mobile network and develop value added service for satisfying different users and applications with different degree of security. The users can easily enjoy secure communication under the general security policy. The general security policy is developed with three layers. One layer is super security policy as value added service that safeguards mobile communication with sensitive information. The second layer is baseline security policy as prevalent service which satisfies essential mobile communication without sensitive information. The last layer is no security policy defined as the policy under which both mobile terminal and application service provider have no security-related function.

1 Scope

This baseline document of x.msec-3 provides a specification of general security policy for secure mobile end-to-end data communication within the framework and requirements of X.1121.

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.

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

[2] ITU-T Recommendation X.803 (1994), *Information Technology – Open Systems Interconnection – Upper Layers Security.*

[3] ITU-T Recommendation X.810 (1995), *Information Technology – Open Systems Interconnection – Security works for Open Systems: Overview.*

[4] ITU-T Recommendation X.805 (2003), *Security Architecture for Systems Providing End-to-End Communications.*

[5] 3GPP, TS 21.133 V4.1.0 (2001), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Threats and Requirements (Release 4).*

[6] 3GPP, TS 33.102 V.5.2.0 (2003), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 5).*

[7] 3GPP, TS 33.203 V.5.2.0 (2004-03), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Access security for IP-based service.

[8] RFC3329 Security Mechanism Agreement for the Session Initiation Protocol (SIP). J. Arkko, V. Torvinen, G. Camarillo, A. Niemi, T. Haukka. January 2003. (Format: TXT=51503 bytes) (Status: PROPOSED STANDARD)

3 Definitions

3.1 The ITU-T draft Recommendation of X.1121 definitions:

3.1.1 Security requirements for mobile user's point of view

- Identity management
- Data confidentiality
- Data integrity
- Authentication
- Access control
- Non-repudiation
- Anonymity
- Privacy
- Usability
- Availability

3.1.2 Security requirements for ASP's point of view

- Data confidentiality
- Data integrity
- Authentication
- Access control
- Non-repudiation
- Availability

3.1.3 Definition of entities

a) mobile terminal;

b) mobile network;

c) mobile user;

d) application service;

e) application server;

f) application service provider;

g) mobile security gateway;

3.2 Additional definitions

3.2.1 Security policy server

Security policy server is an entity that connects to application server or mobile security gateway. It takes security policy management for the application server or mobile security gateway.

3.2.2 Service provider

As an entity offering service to mobile user, service provider includes not only network operator but also application service provider.

3.2.3 Security policy

Security policy is the set of criteria for the provision of security services. The criteria are driven by security requirement, and should be abided by network entities.

General security policy defines the handling tactics of all kinds of application's security requirement in mobile communication environment. From the user's point of view, security policy provides friendly interface of security service to mobile user. Users can easily customize security service for different application scenarios. From the service provider's point of view, security policy makes it possible account for value added security service. Service provider can quickly adapt security technologies as market needing.

Security policy has three basic requirements involving completeness, correctness and consistency. Firstly, the defined policy should cover all the defending targets proposed by different kinds of security requirement; secondly, the defined policy should be practicable, namely, it does not contract with the experience; thirdly, there shouldn't have any policies conflicts, which may result in different decisions when applied to mobile communication.

3.2.4 Security element

ITU-T Recommendation X.805 (2003) identifies eight dimensions that protect against all major security threats, including Access control, Authentication, Non-repudiation, Data confidentiality, Communication security, Data integrity, Availability, and Privacy. Each dimension satisfies certain kinds of security requirement. They can be configured with detailed security technologies and protocols. Such configured security dimension set is named by security element.

3.2.5 Security element combination

As a layer of security policy, security element combination includes a set of security elements. It is used to meet the need of a particular kind of security requirement.

3.2.6 Assets

Assets are valuable properties to be protected by mobile terminal or application service provider. Assets are divided into three kinds of assets; information asset, service asset, and system assert.

3.2.7 Security manager

Security manager is a person or entity that decides the security policy level, manages the set of security policy, and performs security policy-related tasks in the mobile terminal or application service provider.

4 Abbreviations

ASP	application service provider

5 Security policy

It is necessary to establish a general security policy in secure mobile end-to-end data communication. Reasons are described as follows:

5.1 Rigorous mobile environment

Various services provided through mobile network are increasing sharply. The amount of mobile users all around the world also grows remarkably. Being similar with wire network, the mobile network is also threatened by various attacks. Moreover, mobile environment has many limitations such as limited computing power in wireless devices, inadequate memory space, low network bandwidth, and restrictions imposed by underlying communication protocols and services. By this means, effective service with mobile network is more difficult than that with wire network. As the purpose of security policy is to organize various security technologies together to achieve certain degree of security for various services, a general security policy is necessary for the effective service with the rigorous mobile environment.

5.2 Additional investment for security

Comparing with unsecured network, the security network means additional investment from the service provider's point of view. Moreover, there has no absolute security network. The investment on security strongly relies on the degree of security the network can achieve. The additional investment at least includes network management about security, security devices, additional consumption on bandwidth and computing power, the training for security managers and users, etc. Evidently, security is a kind of service that needs a large amount of investment. Thus, it is impossible to provide all the security service without charging. Service providers should find out effective methods to take high security service as value added service. A general security policy can help service providers realize it.

5.3 Various secure algorithms and protocols in different types of terminals.

A variety of security algorithms and protocols exist in different types of terminals. A rigorous problem is how to organize them to provide not only enough degree of security, but also fully interoperation among different types of mobile terminals. The problem can not be solved without an effective security policy. A general mobile network includes various types of terminals. It is necessary to develop a general security policy in both terminal and server ends that can satisfy the security requirements of mobile network effectively.

5.4 Different degree of security for various users and applications

Although security communication is important in many applications, such as e-commerce, etc, many other applications just require low level of security, such as accessing to Internet for open information. In this case, the unidirectional authentication from service to user may be enough. Therefore, the degree of security varies for different users and applications. Service providers should provide different degree of security service to users. A general security policy is necessary to provide the different degree of security. By this means, it is important to consider the general security policy for better service.

5.5 Simple and effective security management for users

Security management is of critical importance in network security. For example, a network that installs many advantage security devices and implements perfect security solution is totally unsecured without effective security management. For the mobile network, besides the professional security managers in the server end, all the mobile users should also take charge of security in terminal end. If any end of the security management fails, the communication is unsecured. As we know, it is impossible to require all the users having much knowledge of security management. Thus, for better service, it is necessary to develop an effective secure policy as simple as possible in terminal end and most policy decisions are done in the server end.

6 Security policy classification

6.1 Types of asset in the mobile environment

The security in the mobile environment protects the asset from attacker. It needs to consider identifying the assets in both mobile terminal and application service provider, which are protected by the classified security policy agreed or pre-shared by two corresponding entities via an in-band channel or out-of-band channel, respectively.

Assets are defined as valuable properties that should be protected by mobile terminal or application service provider. In order to negotiate the security policy between mobile terminal and application service provider, we should first identify the assets to be protected by some sorts of security mechanisms. Assets in the mobile communication context can be grouped into three types of assets; an information asset, a system asset, and a service asst. The system asset and service asset are of the stationary asset, as theses asset would be usually unchanged after setup. However, the information asset is a dynamically managed asset, because it is created, removed, modified, or deleted according to the policy of mobile terminal and application service provider. An information asset could be stored in a system asset and could be manipulated by a service asset. A service asset can be created, deleted, or managed by using a system asset. Table 1 describes the description of assets with examples. All these three types of assets should be protected according to the appropriate security policy negotiated or pre-agreed between the mobile terminal and application service provider. We will focus on only information asset in this recommendation.

Table 1. The classification of assets

Class	Description	Example
Information asset	Valuable data that can be stored, processed, or transferred by computational systems.	Sensitive data, E-transaction data, Business plan
Service asset	Application program that offers the manipulation of data to users.	Web service E-mail service
System asset	Physical hardware components for supporting services and data processing.	File server Telnet server

6.2 Security policy layer

6.2.1 Framework of security policy layer

The category of security policy is divided into two categories: The first category is the security policy group related to the host or domain and second category is a security policy group with a various sensitivity level of asset. Security level should be assigned to hosts or domains that contain assets by using some criteria by mobile terminal and application service provider. Sensitivity level is assigned to assets to be protected by our model.

However, the security policy may be applied to only asset to be protected by mobile terminal and application service provider. But, it is preferable to establish the security policy for context of mobile domain and host, to apply them to all kinds of assets; service asset, system asset, and information asset. If the security policy is negotiated online, the integrity and authenticity of security policy sent from application service provider to mobile terminal or vice versa should be assured via some security mechanisms: digital signature, message authentication code, and pre-shared secret.

Although the classification of security policy and the number of security policies, security level, should be set up by the mobile terminal and application service provider, the reference model may be very helpful to the security manger to make their own policy. Fig.1 proposes typical example to illustrate the framework of security policy in the mobile end-to-end data communication.

Fig.1 shows three security policy layers, which consist of super security policy, baseline security policy and no security policy. Again, the super security policy layer can be grouped into several subgroups of security policies. However, the number and level of security policy groups should depend on the policy of each entity. The more security subgroups of each security sub-layer are desirable to allow the mobile system more available. Therefore, it is preferable to allow both the mobile terminal and the application service to set up the acceptable security policies including the number of security policy subgroup and security policy level.

General security policy for mobile end-to-end data communication shows below:

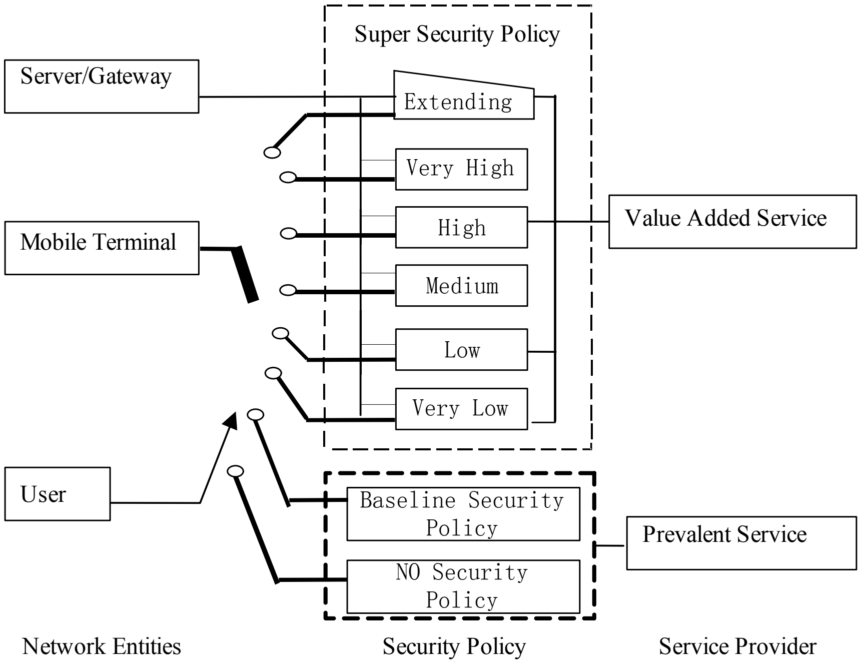

Figure 1 Framework of security policy layer for mobile end-to-end data communication

There are three parts in the illustration of the general security policy. The first part is network entities involving sever/gateway, mobile terminal, and user. The second part, named security policy, is divided into three layers, super security policy, baseline security policy and no security policy. The third part is service provider that provides two types of security services, *i.e.*, prevalent service for baseline security policy and no security policy, and value added service for super security policy. Evidently, from the service provider's point of view, the security policy is indispensable to organize network entities for security service.

- Server/Gateway

  Both baseline security policy and super security policy are available for a communicating process.

- Mobile Terminal

  Only one of groups among low of super security policy, very low of super security policy, medium of super security policy, high of super security policy, very high of super security policy, extending of supper security policy, baseline security policy, and no security policy are available for a communicating process.

- User

  Select a security policy in mobile terminal for a communication process according to the sensitivity of transmitted information.

6.2.2 No security policy as prevalent service

No security policy is defied as the policy under which mobile terminal and application service provider have no security-related function.

In some application, it may not require any security functions. The security of mobile terminal and application service provider with no security policy depends on the security that is provided by network or some other means. But, it is recommended that at least baseline security policy should be assigned to mobile terminal and application service provider in order to assure the secure communication between mobile terminal and application service provider.

6.2.3 Baseline security policy as prevalent service

Baseline security policy is required for all data communication. Thus, it can be considered as prevalent service that the service providers provide. The mobile network should support the baseline security policy that cannot be disabled by both users and the service providers. It only provides enough protection for accounting. Users can use baseline security policy to get open data information from servers.

According to the security requirements from both user's and ASP's point of view that are discussed in the ITU-T recommendation of X.1121, some of them belong to the requirements that the baseline security policy should realize. They are listed as follows:

- Unidirectional Authentication
- Identity management
- Usability
- Availability

In order to process accounting, unidirectional authentication processes from server to mobile terminal, and from mobile terminal to user are provided. The accounting is a basic requirement for service providers. On the other hand, identity management is necessary for authentication.

6.2.4 Super security policy as value added service

Except the security requirements for the baseline security policy, all the other security requirements should belong to super security policy provided as value added service. The security requirements include, but are not limited to:

- Authentication
- Confidentiality
- Integrity
- Anonymity
- Access control
- Non-repudiation
- Privacy

The mobile providers should define several groups of security policy that correspond to users and applications with different degree of security, especially for terminals with limited computing power. Users can easily select suitable group of security policy according to the importance of interactive data before communication begins. Different groups of security policy correspond to different price of added value service.

The mobile terminals should at least support the following three basic groups listed as follows:

- Very High
- High
- Medium
- Low
- Very Low
- Extending

The group of “Very High” means the highest degree of security that can be provided to the users. The service providers can use stronger cryptogram algorithm and longer key length to achieve it. It always consumes much more computing powers on both terminal device and server. Thus the service price of “Very High” security should be the highest. And “Very Low” group indicates that the data communication is only protected weakly. “Extending” group describes the security enforcement that can be combined agilely.

Table 2 presents the description of criteria for assigning security level to each domain/host and asset. Each sub-layer of super security policy should be classified as five subgroups, very high, high, medium, low, and very low. This security policy level could be assigned according to policy by mobile terminal and application service provider. As it is too complex and difficult to make unified unique security sub-layer, careful investigation is required to determine the appropriate security policy. Therefore, the typical example of criteria to assign the security policy level to assets is very useful to security manager.

Table 2 The criteria for assigning the security policy subgroup to assets

Grade	Safety level (for domain & host)	Sensitivity level (for asset)
Very high (+2)	There exists documented organization’s security policy. Appropriate security measures are applied to organization’s network. Incident response process is prepared. Regular security monitoring is performed	If the asset is destroyed, forged or exposed, it will cause a long-term discontinuity of organization’s task. If the asset is damaged, it cannot be recovered.
High (+1)	There exists documented organization’s security policy. Appropriate security measures are provided against known attacks. Regular security monitoring is being performed.	If the asset is destroyed, forged or exposed, it will cause a short-term discontinuity of organization’s task. If the asset is damaged, it can be recovered.
Medium (0)	Appropriate security measures are applied against known attacks. Regular security monitoring is being performed.	If the asset is destroyed, forged or exposed, it will cause temporal inconvenience of organization’s task. If the asset is damaged, it can be recovered.

Low (-1)	Appropriate security measures are applied against known attacks. Irregular security monitoring is being performed.	Although the asset is destroyed, forged or exposed, there will be little effect on organization’s task. If the asset is damaged, it can be recovered.
Very low (-2)	There exist no security measures.	Although the asset is destroyed, forged or exposed, there will be no effect on organization’s task.

Service providers can regulate security technology used in every group as market needed. Moreover, with the development of security technology and different types of terminals, the technical contents in a group may be different with the time being. However, the definition of groups according to the degree of security can give users a uniform and stable solution to enjoy security service. Users needn’t know the detail security technology used in every group. They care only the relationship between different application environments and the different groups of security policy. Before the establishment of data communication, users need only do simple judgement and decision. For example, they can simply use the baseline security policy with which they needn’t do any selection. They can also select one of above groups to begin communication according to the importance of data.

7 Security policy interworking for mobile end-to-end data communication

Before describing secure mobile technologies, models of mobile end-to-end data communication should be defined. Model of mobile network environment will clarify the relationship between network entities and the secure mobile technologies that should be adapted.

7.1 Reference Model of security policy for mobile end-to-end data communication

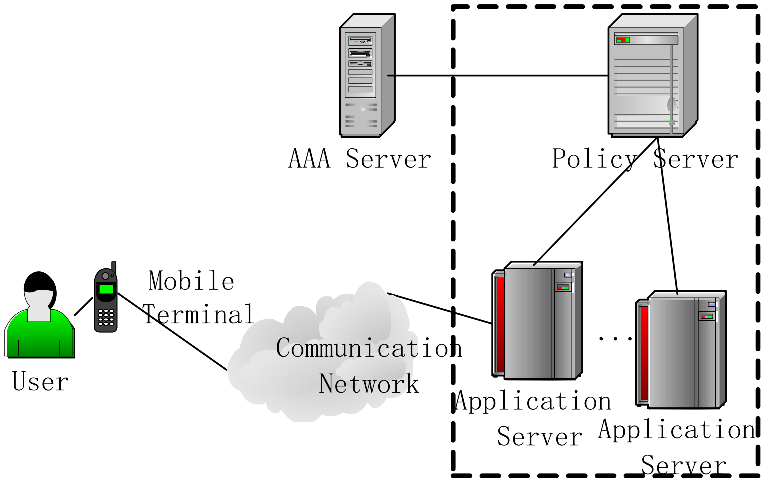

Figure 2 –Model of security policy for mobile end-to-end data communication

Security policy server is added to original model of mobile end-to-end data communication. Fig.2 depicts the reference model of security policy for mobile end-to-end data communication.

There are six entities in this model: mobile user, mobile terminal, communication network, application server, security policy server, and AAA server.

There exist four relationships in this model: relation between user and mobile terminal, relation between mobile terminal and application server, relation between application server and security policy server, and relation between policy server and AAA server. Interworkings among network entities will be described in the following sections.

7.2 Interworking between mobile user and mobile terminal

Mobile user chooses security level for application before communication starts. Security elements compose security level that is used to safeguard the application.

7.3 Interworking between mobile terminal and application server

Mobile terminal negotiates with application server about security level and detailed configuration of security elements. Information on security level and security element list is sent to application server. Both sides make agreement with security elements, technologies and protocols bilaterally supported.

7.4 Interworking between application server and security policy server

The result of negotiation for security level and detail information on security elements are transferred from application server to security policy server. The latter evaluates the result and returns the price of security service to the application server. Mobile user and application server confirm whether the service accepts the price. If they do accept the price, later communication will share the chosen security protection. Rejecting the bidding of security policy server, they can re-book the security level and initiate the negotiation again.

Both application server and security policy server are logical units. One policy server maybe manages several application servers, decided by the scale of service and ease of management. The application server communicates with security policy server via secure charnel. Application server provides different services for mobile user, managed and owned by ASP. Security policy server stores policy information on classification and configuration, evaluates security level, and collects accounting information on security service. Policy server is maintained by security manager.

7.5 Interworking between security policy server and AAA server

Application server sends AAA server the unit price of security element and accounting information. The latter involves security level, configuration of security element, starting and ending time of communication, and flow and service times. Having received them, AAA server prices the security service.

8 Functions of security policy for mobile end-to-end data communication

This function split divides security policy into some security levels. Each level provides different degree of security service for application. Security manager makes rules for the classification of security level.

Five network entities have operational functions in the security policy model of mobile end to end data communication. These network entities include mobile user, mobile terminal, application server, security policy server, AAA server. Operations on the interface among the entities are divided into five categories, such as classification of security level, configuration of security level, negotiation of security level, accounting of security service, and call of security resource.

8.1 Classification of security policy

General security policy for mobile end to end data communication has a four-layered hierarchy shown in fig.3.

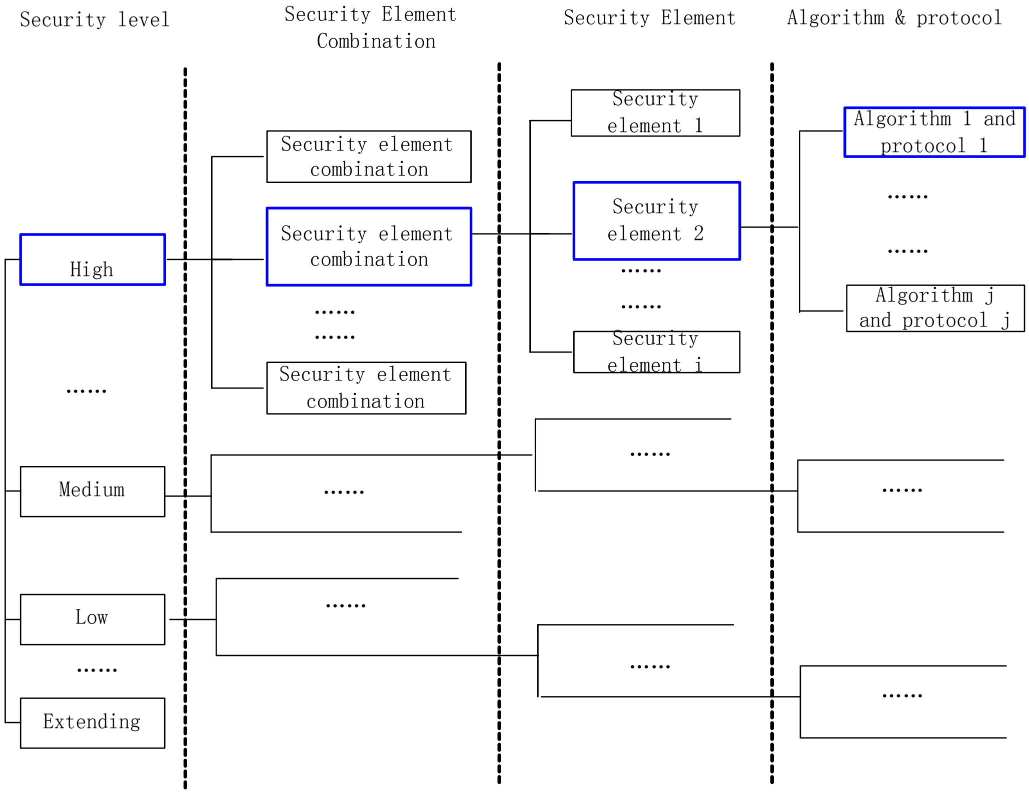
Security level
Security Element Combination
Security Element
Algorithm & protocol
High
……
Medium
Low
……
Extending
Security element combination
Security element combination
……
……
Security element combination
……
……
Security element 1
Security element 2
……
……
Security element i
……
……
Algorithm 1 and protocol 1
……
……
Algorithm j and protocol j
……
……

Figure 3 Hierarchy of General Security Policy

8.1.1 Classification of Security level

Security level is the first layer of security policy. Classification of security level is set up by security manager basing on security requirement as market need. Finely defined security level should provide security service with different degrees. With these labels, mobile user can easily explore security service for some security critical applications. Policy server, application server and mobile terminal share the same classification of security level.

8.1.2 Classification of Security element combination

Security manager should refine the protection objective in each security level, and fulfill work of designing the different security suite to meet the need of security requirement in one security level. As the second layer of security policy, security element combination is used to describe and meet the need of a particular kind of security requirement. There may exist several security element combinations in one security level.

8.1.3 Classification of Security element

Basing on the protection objective, Security elements are selected to fill in the security element combination. As the third layer of security policy, security element depicts different kinds of dimensions of security considerations, such as authentication, data confidentiality and data integrity etc. A union of security elements as a whole describes concrete security requirement.

8.1.4 Classification of Algorithm and protocol

The last layer of security policy relates to detailed protocols and algorithms. Each security element is bound with a certain kinds of algorithms and protocols. That is, security mechanisms for every security element will be appointed definitely. Mobile terminals and application server may support different algorithms and protocols. They should share some common information on the identifier of supported algorithms and protocols.

8.2 Configuration of security policy

The content used to configure the different degree security level is divided into four folds, including:

(1) List of identifiers for security level,

(2) List of identifiers for security elements combination,

(3) List of identifiers for security elements,

(4) List of identifiers for security algorithms and protocols.

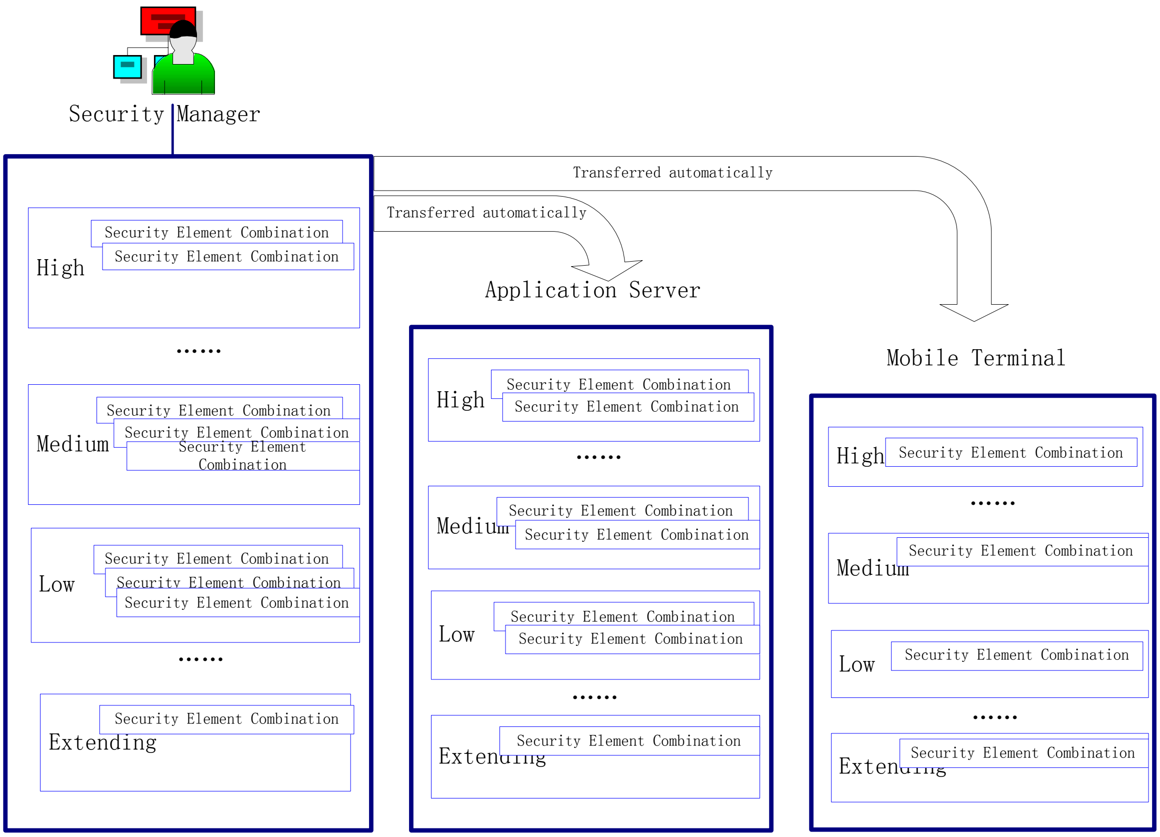
Security Manager
Transferred automatically
Transferred automatically
Application Server
Mobile Terminal
High
Security Element Combination
Security Element Combination
……
Medium
Security Element Combination
Security Element Combination
Security Element Combination
Low
Security Element Combination
Security Element Combination
Security Element Combination
……
Extending
Security Element Combination
High
Security Element Combination
Security Element Combination
……
Medium
Security Element Combination
Security Element Combination
Low
Security Element Combination
Security Element Combination
……
Extending
Security Element Combination
High
Security Element Combination
……
Medium
Security Element Combination
Low
Security Element Combination
……
Extending
Security Element Combination

Figure 4 Configuration of Security Policy

8.2.1 Configuration of Security level for security policy server

Security manager decides security elements according to market demand. Every security elements have different security capability. For the Fixed security levels, security element combination is configured to different security degrees. Then security manager configures security elements in the combination with special security algorithms and protocols. For the customized security levels, policy server dose not know which security elements, detailed security algorithms, and protocols are configured in security level by user. Therefore, security manager should configure all possible security elements in line with security algorithms and protocols.

8.2.2 Configuration of Security level for application server

Configuration of security level for application server is obtained from security policy server.

According to security requirement, For the Fixed security levels, security manager selects proper security element combinations from the policy server's security element combination of each security level, and applies them to corresponding security level of the application server. Also, security manager selects several proper algorithms from policy server's security algorithm in line with different security element, and applies them to related security elements of application server. For the customized security level, configuration is the same method as used in policy server.

8.2.3 Configuration of Security level for mobile terminal

Configuration of security level for mobile terminal shares the similar process to the configuration of application server. Information on configuration is transferred from security policy server to mobile terminal.

Security level of mobile terminal is configured according to its application scope and characteristic. For Fixed security levels, security manager selects proper security elements from the policy server's security element combination of each security level, and applies them to corresponding security level of the mobile terminal. According to the requirement, security manager selects several proper algorithms from policy server's security algorithm corresponding to different security elements, and applies them to related security elements of the mobile terminal. For the customized security level, it is configured by mobile user. There is only one security element combination, which includes the security elements specified by user.

8.3 Negotiation of security policy

The security policy for context around the application server and mobile terminal is very important to provide the secure end-to-end data communication. The mobile terminal and application service provider may negotiate the security policy for asset and the policy for context via online or out-of-band, because the security policy around the mobile terminal and application service provider affect the security service directly.

Security policy management at both mobile terminal and server ends is asymmetric. The negotiation between them is not a peer-to-peer process.

At the mobile terminal end, simple security policy can be configured manually by user. For example, user can simply select one item among High, Medium and Low as needed to finish the security policy configuration for a particular application.

However, it is necessary to add a security policy server to execute complex security management at the server end. The security policy server should analyse the security technology from the mobile terminal and try to understand the security protocols that the mobile terminal supports. It should also evaluate the degree of security with different compositions of security protocols. Security policy server can decide among acceptance, rejection and conditional acceptance of the connection. The detail of conditional acceptance can be configured in security policy server.

Negotiation between mobile terminal and application server makes agreement with detailed information on security elements, including security algorithms and protocols.

8.3.1 Contents of negotiation

The following information are included in the result of negotiation operation, such as

(1) List of identifiers for security level,

(2) List of identifiers for security elements combination,

(3) List of identifiers for security elements,

(4) List of identifiers for security algorithms and protocols.

There maybe some difference between negotiation result and mobile user's selection of security policy, for the very reason that the security algorithms and protocols should be supported by both application server and mobile terminal.

8.3.2 Procedure of negotiation

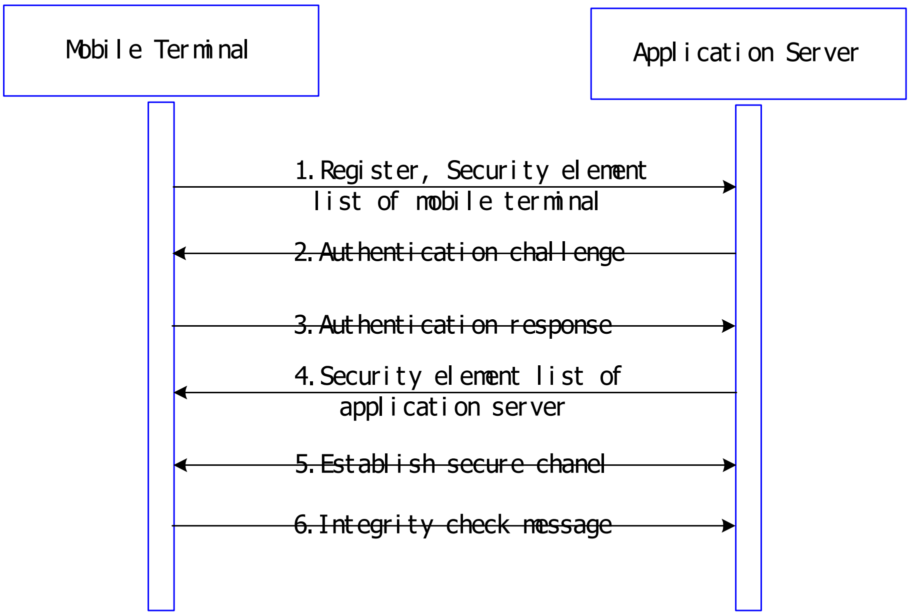
Mobile Terminal
Application Server
1.Register, Security element list of mobile terminal
2.Authentication challenge
3.Authentication response
4.Security element list of application server
5.Establish secure chanel
6.Integrity check message

Figure 5 Negotiation of security policy

The procedure of negotiation includes six major steps as follows, shown in fig.5.

(1) Before a mobile terminal can get access to application server, at least its Public Identity need to be registered and its Private Identity be authenticated. In order to get register, the mobile terminal sends a REGISTER message toward application server。 It also sends a list of identifiers for security elements combination and lists the integrity and encryption algorithms, which are supported by mobile terminal.

(2) Upon receiving the REGISTER message, application server shall send an authentication challenge to the mobile terminal by using an Authentication Vector, which is used to authenticate and agreeing keys with the mobile terminal.

(3) Mobile terminal authenticates application server. After a successful authentication, mobile terminal computes the session keys and sends an authentication response to application server.

(4) Application server authenticates mobile terminal. If authentication is successful, application server sends a list of identifiers for security elements combination and lists the integrity and encryption algorithms, which are supported by application server.

(5) The strongest algorithms supported by both sides will be chosen. Then a secure channel will be established by mobile terminal and application server.

(6) Mobile terminal sends negotiation messages to Application server. The messages' integrity and confidentiality will be checked by the server. After successful checking, application server sends mobile terminal a message to indicate the success. The negotiation procedure is aborted, if those checks fail.

8.4 Accounting of security service

8.4.1 Function definition

This functional split responds for translating accounting information into formal format recognizable for AAA server. Application server send accounting information to security policy server. Such information includes starting/ending time of communication, traffic measurement data, and request times of security service. Security policy server controls security service.

8.4.2 Requirement for AAA server

AAA server should provide accounting utilities for the following data, such as communication time, the quantity of traffic, service time, etc.

8.5 Call of security resource

This functional split relates to how to utilize security technology and resource to protect current communication. Security policy server controls the starting and ending time of calling security resource. Authentication, encryption, and digital signature may be called according to selected security service.

Appendix A: Example of security mechanism in line with subgroup of security policy

Key distribution/sharing is needed for data confidentiality, authentication. Table 3 describes the typical security mechanism corresponding to each security element. The list in the last column of Table 3 is of little significance, that is, NOT mandatory option, and it can be only used as a guideline for security manager to determine and their own security policy. The any other security algorithms with the equivalent cryptographic strength or key length are available, only if they are one of the algorithms chosen by security manager for specified application. The specific security mechanism of each security element is assigned by a security manager of the application service provider.

Table 3 Typical security mechanisms corresponding to a subgroup of security policy

Security requirement	Security functions/security policy subgroup		Typical security mechanisms
Data confidentiality	Encipherment/ decipherment	Very high	AES-256, RSA-2048
		High	-
		Medium	AES-128, RSA-1024
		Low	-
		Very low	DES-64
Data integrity	Hash function	Very high	SHA-384
		High	-
		Medium	SHA-160
		Low	-
		Very low	MD5-128
User authentication	Authentication exchange	Very high	Bilateral authentication with GQ-2048
		High	-
		Medium	Bilateral authentication with GQ-1024
		Low	-
		Very low	Bilateral authentication with GQ-512
Data origin/receipt authentication	MAC	Very high	MAC with SHA-384
		High	-
		Medium	MAC with SHA-160
		Low	-
		Very low	SHA-MD5-128
Non-repudiation	Digital signature	Very high	DSA-2048
		High	-
		Medium	DSA-1024
		Low	-
		Very low	DSA-512
Key Exchange	Key Exchange protocol	Very high	DH-2048
		High	-
		Medium	DH-1024
		Low	-
		Very low	DH-512
Access control	Access control mechanism	Very high	PMI (Privilege Management Infrastructure)
		High	-
		Medium	RBAC
		Low	-
		Very low	MAC