中 原 大 學
電機工程學系
碩士學位論文

3G 行動通訊使用者認證協定之研究

A Study on Authentication Protocol for 3G Mobile Communication Systems

指導教授：涂世雄

研 究 生：林志興

中華民國九十一年六月

博碩士論文授權書

(國科會科學技術資料中心版本 91.2.17)

本授權書所授權之論文為本人在__ 私立中原 __大學(學院)__ 電機工程學 __系所__通訊 __組__九十__學年度第 二 學期取得__碩 __士學位之論文。

**論文名稱：__3G 行動通訊使用者認證協定之研究 **

☑同意 □不同意 (政府機關重製上網)

本人具有著作財產權之論文全文資料，授予行政院國家科學委員會科學技術資料中心、國家圖書館及本人畢業學校圖書館，得不限地域、時間與次數以微縮、光碟或數位化等各種方式重製後散布發行或上載網路。

本論文為本人向經濟部智慧財產局申請專利(未申請者本條款請不予理會)的附件之一，申請文號為：_____，註明文號者請將全文資料延後半年再公開。

☑同意 □不同意 (圖書館影印)

本人具有著作財產權之論文全文資料，授予教育部指定送繳之圖書館及本人畢業學校圖書館，為學術研究之目的以各種方法重製，或為上述目的再授權他人以各種方法重製，不限地域與時間，惟每人以一份為限。

上述授權內容均無須訂立讓與及授權契約書。依本授權之發行權為非專屬性發行權利。依本授權所為之收錄、重製、發行及學術研發利用均為無償。上述同意與不同意之欄位若未鉤選，本人同意視同授權。

指導教授姓名:涂世雄

研究生簽名: 學號:8978043

(親筆正楷) (務必填寫)

日期:民國 九十一年六月二十六日

---

1. 本授權書 (得自 http: //nr.stic.gov.tw/theses/html/authorize.html 下載) 請以黑筆撰寫並影印裝訂於書名頁之次頁。
2. 授權第一項者，請確認學校是否代收，若無者，請個別再寄論文一本至台北市(106-36)和平東路二段 106 號 1702 室 國科會科學技術資料中心 王淑貞。(本授權書諮詢電話:02-27377746)
3. 本授權書於民國 85 年 4 月 10 日送請內政部著作權委員會(現為經濟部智慧財產局)修正定稿，89.11.21 部份修正。
4. 本案依據教育部國家圖書館 85.4.19 台(85)圖編字第 712 號函辦理。

簽署人須知

1. 依著作權法的規定，任何單位以網路、光碟與微縮等方式整合國內學術資料，均須先得到著作財產權人授權，請分別在兩種利用方式的同意欄內鉤選並填妥各項資料。我國博碩士論文八十二學年度以前摘要資料庫及八十四學年度以後全文資料微片目錄資料庫已上載於行政院國家科學委員會科學技術資料中心網站www.stic.gov.tw, 七十三學年度以後摘要資料庫已上載於教育部國家圖書館網站 www.ncl.edu.tw。

2. 所謂非專屬授權是指被授權人所取得的權利並非獨占性的使用權，授權人尚可將相同的權利重複授權給他人使用; 反之即為專屬授權，如果您已簽署專屬授權書予其他法人或自然人，請勿簽署本授權書，著作人日後不可以主張終止本授權書，但您仍可授權其他法人或自然人上述的行為。

3. 全國博碩士論文全文資料整合計畫的宏觀效益:

在個人方面，您的論文將可永久保存(微縮技術在理論上可保存八百年，實證已逾百年)，也因為您的授權，使得後進得以透過電腦網路與光碟多管道檢索，您的論文將因而被充分利用。在國家總體利益方面，紙本容易因影印而造成裝訂上的傷害，圖書館中孤本的公開陳列與外借也有破損之虞，唯有賴政府全面性的整合，借助科技設備才能一舉完成保存與利用的全方位效益，回憶您過去尋找資料之不便經驗，學弟與學妹確實須要您的論文與授權書。

中原大學碩士班研究生

論文口試委員審定書

第 九十 學年度第 二 學期

電機工程 學系 研究所 林志興 君所提之論文

題目：(中文)3G 行動通訊使用者認證協定之研究

(英文) A Study on Authentication Protocol for 3G Mobile Communication Systems

經本委員會審議，認為符合碩士資格標準。

學位考試委員會 召集人 _____

委員 _____

委員 _____

委員 _____

委員 _____

委員 _____

指導教授 _____

系(所)主任 _____

中華民國 九十一年六月二十六日

20P029-051

摘要

近幾年來，由於行動通訊技術發展迅速，帶給我們生活上許多便利與好處，例如：可以利用手機上網、進行電子交易、下載電子地圖、收發電子信件、視訊會議等等。在存取這一些服務時會有大量的重要訊息在無線通道中傳遞，如此會造成有心人士對這一些資料進行擷取或竊聽的動作，因此，我們必須考量到重要訊息在無線通道中傳輸的安全問題。在本論文中，我們提出新的三個基於公開金匙密碼系統的認證機制。所提出的三個認證機制是用來解決第三代行動通訊的安全問題，在安全性方面也比傳統式密碼系統來的安全。在第一個認證架構中，是使用者擁有網路運作者的公開金匙，網路運作者也擁有使用者的公開金匙。在第二個認證架構中，是利用交換使用者與網路運作者雙方證書的方法，去達成互相交換彼此的公開金匙。在第三個認證架構中，是藉由證書服務者發證書給使用者與網路運作者，藉由這一些證書來獲得雙方的公開金匙。在此，我們針對第三代行動通訊系統所提出的認證機制，是被分析能夠達到安全性的需求與威脅的準則與目標。此外，也能夠達到較低的運算複雜度和設計簡單但足以符合安全性認證協定。

誌謝

本論文得以順利完成，最重要是感謝指導教授涂世雄老師給予學生在研究所求學其間，不論是在專業知識領域的細心指導以及待人處事的態度等等，均給予學生極大的啟示與收穫，在此學生衷心地表達最誠摯的謝意，同時並感謝口試委員黃教授正光、張教授富爵，對本論文提供寶貴的建議與指導。

我特別要感謝我的家人，尤其是我的父母親，他們的支持與鼓勵是促使我完成學業的最大動力泉源，也要感謝姊姊與敦裕姊夫給予我課業上與精神上的幫助。此外，還要特別感謝張黃道學長給予我專業知識上的指導與幫助，以及感謝獻文同學在我研究所生涯帶我許多的快樂與幫助、震寰同學給予我電腦方面知識的幫助與討論、家維與晉弘同學在生活處事上的關懷，以及感謝學弟乃仁、昱宏、俊茂、宗驥、志昇以及瑋志一年的相處也帶給我很多的快樂時光。最後，將本論文獻給所有愛護與關心我的人。

目 錄

第一章　簡介

近年來行動通訊發展迅速，從以前第一代類比式行動通訊至第二代數位式行動通訊，最後發展到現在的第三代行動通訊，其發展帶給人類無限的便利，人們使用電話通訊不再受地點時間的限制，只要能在網路系統涵蓋範圍，即可隨時隨地的進行通訊。就第三代行動通訊所提供的服務包含：語音影像網際網路的服務電子郵件電子商務等等。在無線通訊的過程中，重要的資訊傳輸在一個不安全的通道，因此我們需要建立一個安全的通訊協定來確保通訊過程中的安全，而此通訊協定成為安全行動通訊系統中不可或缺的重要一環。

在本論文中，我們主要的研究方向是針對第三代行動通訊系統的安全需求來建立新的認證協定，以解決通訊過程中資訊傳輸不安全的問題。

詳見英文附錄

第二章 回顧第二代行動通訊協定之技術與針對第三代行動通訊之 UMTS 安全需求之考量

本章介紹一些在通訊認證技術的一些專有名詞。首先，介紹第二代行動通訊的認證協定的運作方式如：GSM，在第三代行動通訊系統方面，我們介紹由西門子所提出的三種認證協定的運作方式。最後，我們將介紹在設計第三代行動通訊認證協定時所必須要遵循的一些設計法則與一些安全上的需求。

詳見英文附錄

第三章 第三代行動通訊認證協定之研究成果

在本章中，我們提出了三個都是基於公開金匙密碼系統的認證機制來達成，在第一個機制中，雙方都擁有對分的公開金匙來進行通訊。在第二個機制中，雙方並沒有對方的公開金匙，但是藉由證書來達成交換雙方的公開金匙。在第三個機制中，藉由證書服務者來提供證書給使用者與網路運作者，使用者與網路運作者利用證書服務者所發的證書來獲得雙方的公開金匙。並且我們利用新的訊息流程法來表示新的認證協定機制，讓我們更加瞭解在每一步的傳輸過程中，每一個資料所代表的意義與關係。我們針對第三代行動通訊系統所提出的認證機制，是被分析能夠達到安全性的需求與威脅的準則與目標。此外，也能夠得到較低的運算複雜度和設計簡單但足以符合安全性認證協定。

詳見英文附錄

第四章 結論

本論文我們提出三種新的認證協定架構來滿足第三代行動通需求，未來我們將針對未來新的行動通訊設計新的認證協定以滿足其安全需求，並且繼續朝向認證協定的架構是否能夠更為精簡，如同：認證通訊的次數與所傳輸的訊息數目。

詳見英文附錄

英文附錄

Contents

Abstract

In this thesis, we propose three new authentication mechanisms based on Asymmetric-key cryptosystems. The three authentication protocols are designed based on the security requirements of the third generation mobile communication systems, which is proposed by UMTS. The advantages of the Asymmetric-key cryptosystems are to solve a very important key management problem for key distribution. Besides, it can provide non-repudiation for the part of the transmitted data. Therefore, we adopt the Asymmetric-key cryptosystems to design our authentication schemes. The characteristic of the first schemes is that the User and the Network Operator have the public keys from each other, respectively. The characteristic of the second schemes is that we exploit the exchange of certificate to achieve the goal of exchange of the public key between the User and the Network Operator. The characteristic of the third schemes is that the Network Operator can obtain the public key from the User's certificate sent by Certificate Server. Similarly, the User can obtain the public key from the Network Operator that is sent be Certificate Server. The proposed authentication protocols for 3G mobile communication systems are analyzed to be correct to achieve the critical goals of the requirements of security and threats, and these protocols are efficient and effective because they are computationally low complexity and are simple but secure enough.

List of Figures

List of Tables

Chapter 1 Introduction

1.1 Authentication and UMTS

In recent years, mobile communication has been developed very rapidly. From the first-generation analog cellular mobile communication to the second-generation digital cellular mobile communication system, and the evolution to the third-generation mobile communication system until now, the usage of mobile and wireless communication systems has become more and more popular and convenient in spread worldwide. Nowadays, the technology of wireless mobile communication is not only beneficial for the customer better voice service but also extends to non-voice service such as image, internet service, computing data, e-mail, e-commerce and so on. People can communicate with others anytime and everywhere. However, people would be faced with the problem of serious security threats because of the openness of wireless communications. Therefore, to provide users a mechanism to protect the privacy between communicating parties is a very important issue. Since the transmission interface of the mobile communication system is through the radio channel, the actions of exchanging the private information of users or systems over insecure communication channels will increase potential threats of security, such as eavesdropping and masquerading legal users [1][2][3].

Besides, the location of a particular mobile user may need to be protected to ensure privacy. Therefore, how to provide very secure measures for protection of our mobile communication environment is very important. Authentication and confidentiality are essential security

services, which aim to verify identities of users to prevent impersonation and to protect private communication against unauthorized eavesdropping, respectively [4].

An authentication protocol is designed to allow participating entities to demonstrate their knowledge of certain secrets, which involve in verifying the identities of both parities over the wireless link and in establishing a common secret key between them. Hence, based on the authentication protocol, we can reduce or even completely eliminate threats that eavesdropping and masquerading legal users.

In general, the participants consist of **Subscribers**, the **Network Operators** and **Service Providers**. The authentication protocol usually has two common elements: (a) communication identities, which can prove their own identities and check the other's identities. (b) A session key, which will be distributed for the consequent communication after the participants have been proved their identity by each other. Among many issues of security [5-11], in general, six characteristics are needed for secure mobile communication system.

a. Any participant involved in the mobile communication systems must have the ability to recognize the true identity of each other.
b. During the transmission process, all of the sensitive information must be encrypted.
c. The mobile communication system must guarantee validity of the transmitted data.
d. The transmitted data cannot be repudiated.
e. The true identity of any participant must be unknown to the

stranger.

f. The mobile communication system must have resistance of relay-type clone attack [5] [12].

The purpose of authentication process is to offer the communicating parties with certain guarantee so that they can identify each other. This process is called the user authentication.

Authentication can be unilateral authentication or mutual. Unilateral authentication is to provide one participant with the verification of the other's identity. Mutual authentication is to provide both participants with verification of each other's identity. Therefore, before a mobile user accesses mobile system services, he should be authenticated by the mobile system if the mobile system has an authentication protocol for transmission of a mobile user's secure information. Furthermore, if we want to transmit the private information to the mobile system by the air-interface, the content of the message can be canceled by encryption. Usage of encryption techniques, before a communication begins, both parties should share a common session key in the secure communication.

The movement of a mobile user and the confidentiality of a mobile user's identity are also the security issues showing up in the mobile communication environment.

The solution of the anonymity and intractability problems is to assign a nonce identity such as alias to the user while he is roaming. In the Global System for Mobile communication (GSM), a temporary mobile subscriber identity (TMSI) is a kind of alias. The Visitor Location Register (**VLR**) assigns TMSI to a mobile user. While a mobile user roaming in the areas, the service is not controlled by user's Home

Location Register (**HLR**) but controlled by the given **VLR**, i.e. only the mobile user and **VLR** know the TMSI.

In the 1990s, several security-related protocols for wireless mobile communication systems have been proposed based on the symmetric key cryptosystems (e.g. DES) or the public key cryptosystems (e.g. RSA) [9-10][14-21]. For symmetric key techniques, both communicating participants share the key. For a public (asymmetric) key technique, where there are two keys: public and private keys. In such case, a participant's private key is only known by itself and both communicating participants know the public keys. However, in mobile communication systems, two major limitations should be considered when the security protocols are designed. First, the low computational power of mobile stations should be considered. It means that a security protocol requiring a great quantity computational on the mobile stations is not realistic. Second, wireless mobile communication is with a lower bandwidth and higher channel error rate than fixed network. Therefore, the security protocols should be designed to minimize the message sizes and the number of message exchanged.

On the 1st July 1991, in a city park of Helsinki, Finland, the first public GSM was created, which is regarded as the second-generation mobile telecommunication. In the past ten years, GSM has become a truly universal mobile communication system. The second-generation systems mainly provide speech services. Hence, ten years later GSM has brought us onto the footprint of the third generation mobile communications system, which is Universal Mobile Telecommunication System (UMTS) in European [22]. The UMTS is designed to provide access to a wide rang

of services. Many of these services and environments in which they will be used are already provided by various existing systems such as cordless, cellular, and satellite. UMTS will provide an integrated system in which users can access the desired service via uniform service access procedures irrespective of the environment they find themselves in. UMTS will provide service involving multimedia services, voice and non-voice service such as audio, video, speech, multimedia data and billing services, surfing the web, e-commerce, e-mail from a mobile user's terminal, electronic postcard, and so on. For the above descriptions of services, because of the various services operated in the hybrid mobile networks, some security issues new for the 3G should be considered particularly. There will be new and different providers of service such as content providers, data service providers, **HLR**-only service providers. 3G mobile systems will be positioned as the preferred means of communications for users. There will be active attacks on users. In active attacks, equipment is used to impersonate parts of the network to actively cause lapses in security. In passive attacks, the attacker is outside the system and listens in, hoping security lapses will occur. Non-voice services will be as important as, or more important than voice service, since the terminal will be used as a platform for e-commerce and other applications.

For the securities of multi-service, there are three key principles behind UMTS securities [5]

1) 3G security will build on the security of second-generation systems. Security elements within GSM and other second-generation systems that have proved to be **needed** and

robust shall be adopted for 3G security.

2) 3G security will improve on the security of second-generation systems. 3G security will address and correct real and perceived weaknesses in second generation systems.

3) 3G security will offer new security features and will secure new services offered by 3G.

Next, we introduce a simplified role model for UMTS in **Figure 1.1**. The role model describes the actions and responsibilities of the participants within relationships.

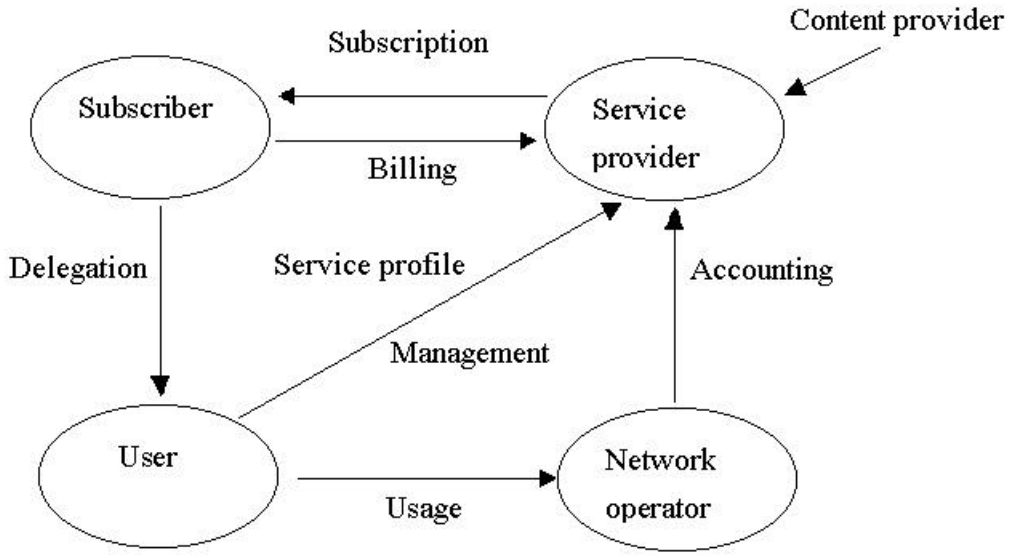

Figure 1.1 .Simplified role model for UMTS

Here, we introduce four actors and the actions between them in **Figure 1.1** [23]. **Subscriber** is a person or an entity that has a contractual relationship with a **Service Provider** on behalf of one or more users. A **subscriber** is responsible for the payment of charges due to that service provider. **User** is a person or an entity authorized is a **subscriber** and uses

services subscribed to by the subscriber. **Service Provider** has overall responsibility for the provision of service or a set of services to users associated with a subscription and for negotiating the network capabilities associated with that service or set of services with **Network operators**. **Network Operator** provides the network capabilities necessary for the support of the services or set of services offered to users.

In the role model, we can find that actions between the actors are transmission of some sensitive data. Therefore, we should take safety measures to them against attacks.

1.2 The Proposed Schemes

In this thesis, we propose three new authentication mechanisms based on Asymmetric-key cryptosystems. The three authentication protocols are designed based on the security requirements of the third generation mobile communication systems.

In most of the authentication protocols, generally the designer sends the all messages included in each transmission step. However it is difficult for us to understand the meaning and the relationship of these messages explicitly. Therefore, we use a representation of message flow to reconstruct the protocol in order to assist us to understand these messages and the relationship in each transmission step.

The advantages of the Asymmetric-key cryptosystems for key distribution solve a very important key management problem. Besides, it can provide non-repudiation for the part of the transmitted data. Therefore, we adopt the Asymmetric-key cryptosystems to design our authentication schemes. In our proposed authentication protocols, they

have more secure than the symmetric-key cryptosystems, and we only use the exclusive OR operation to achieve authentication between the **User** and the **Network Operator**.

1.3 Organization of The Thesis

The thesis is organized as follows. In Chapter 2, we introduce some technologies, which are concerned with the authentication protocols for mobile communication. The end of Chapter 2, we refer the security threats and requirements for the third generation mobile communication systems proposed by ETSI. The three new authentication mechanisms based on Asymmetric-key cryptosystems are described in Chapter 3. In Chapter 4, it includes the brief conclusions and discussions of the direction of our future works.

Chapter 2 Review of the 2G Mobile Systems and Security Considerations for UMTS

In this chapter, we introduce some terminologies about security of the mobile communication environment in section 2.1. We describe some previous researches on the authentication protocols. It includes protocols using in the 2G mobile systems and cryptography, which is protecting information transmitted through public channel. In the cryptography side, which is avoiding illegitimate intruder to eavesdrop the sensitive information, we need a powerful mechanism to ensure security of the system. The powerful mechanism is an authentication protocol. Finally, we will focus on security threats and requirements, which are defined in Universal Mobile Telecommunication System (UMTS).

2.1 Terminology

Authentication should be possible for the receiver of a message to ascertain that this message origin.

Unilateral Authentication provides with the verification of the claimed identity of the participant.

Mutual Authentication provides with the verification of the claimed identity of each of the communicating participants, to each other.

Plaintext is the original message or data.

Encryption is to conceal an original message or data by performs various substitutions and transformation on the original message or data.

Ciphertext is an encrypted message.

Decryption will encrypt message to be the ciphertext and turn it back into plaintext.

Data confidentiality prevents information that is not made available or disclosed to unauthorized individuals, entities or processes.

Location confidentiality prevents the presence or the arrival of communicating participant in a certain area, which cannot be determined by eavesdropping on the radio access link.

Data integrity prevents that data has not been altered in an unauthorized manner.

Key freshness**:** a key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorized party.

Non-repudiation prevents either sender or receiver from denying a transmitted message. Thus, when A sent a message to B, B receives the message that can be proved that the message was in fact sent by A.

Timestamps: If the message contains a message as fresh that, in A's judgment, is close enough to A's knowledge of current time. This approach requires that clocks among the various participants be synchronized.

Challenge/Response is when a party A, excepting a fresh message from B, first sends B a nonce and requires that the subsequent message received from B contain the correct nonce value.

User anonymity is currently provided by use of temporary identities to communication. However, in the case of new registrations, the true identities are necessary.

2.2 Previous Research on Authentication Protocols of the 2G Mobile Systems and UMTS

2.2.1 GSM Authentication Protocol

When a mobile station attempts to access a network, which needs authentication process to ensure that the network service will not be obtained fraudulently. In the following, we review the original GSM authentication protocol [24].

The Global System for Mobile communication (GSM), issued by European Telecommunication Standards Institute (ETSI), was developed during the 1980s [26]. GSM is the first mobile digital cellular system (second-generation mobile system) that providing a broad spectrum of communication capabilities and some digital service of security such as user authentication, signaling traffic confidential, encryption, and roaming, etc..

In the **Challenge/Response** mechanism of GSM authentication protocol [27], each Mobile Station (**MS**) has a unique identity, which is an International Mobile Subscriber Identity (IMSI). IMSI is use to register and choose its own Home Location Register (**HLR**) to register. Between the **User** and the **HLR** with a share key of authentication, K_i. Therefore, in this protocol, it uses three security algorithms, A_3, A_8, A_5, which were authentication function in the GSM system. The function A_3 is a one-way function whose input is the challenge, a random number (RAND), form HLR. Between mobile station and HLR share key K_i, which generate MS's response to **HLR**'s **Challenge**, the simplicity that A_3 is use to authentication MS. The function A_8 is a one-way function,

which uses RAND and Ki to generate a private key Kc. Kc is used for voice and data privacy. The function A_5 is a symmetric-key crypto-function with key Kc, which encrypts transmitted data.

When the MS roams into the mobile system that is not controlled by **HLR**, the Visitor Location Register (**VLR**) will provide the communication service. The following steps in **Figure 2.1**, describe the workflow of security authentication protocol of GSM. We will use a presentation of message flow proposed by [28](see Appendix A), which can assist us in recognizing what the meaning of each message involved in the authentication protocol.

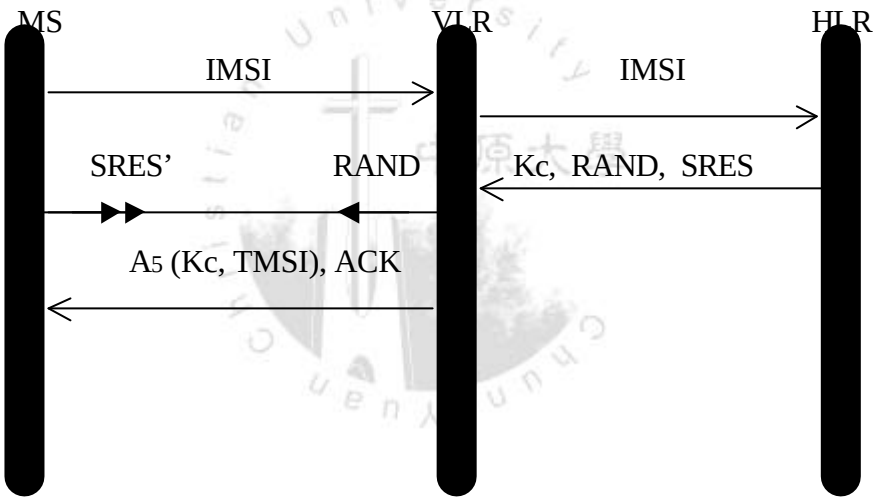

Figure 2.1. GSM authentication protocol

(1) When a Mobile Station (**MS**) attempts to access service from the network, it will transmit IMSI to **VLR**, which is a registration request. The **VLR** obtains the MS' s IMSI and pass it to the **HLR**

(2) **HLR** generates a random number RAND and uses the algorithm A3 to produces SRES and uses the algorithm A8 to produces Kc. Both A3 and A8 choose RAND and Ki as inputs. Then the **HLR** transmits Kc, RAND and SRES to the **VLR**. These messages are

used in to authentication of the **MS**.

(3) The **VLR** receives these messages and forwards the RAND to MS as a **challenge** message. Then the **MS** uses the algorithm A3 to generate a corresponding message SRES'.

(4) **MS** transmits a response message SRES' to **VLR**. When **VLR** receives SRES' from the **MS**, it can verify the SRES from the **HLR** and the SRES' from the **MS**. If they are the same, the **MS** is authenticated.

(5) **VLR** encrypts a temporary TMSI transmitting to **MS** by new session key, which is K_c. TMSI is a temporary identity to **MS** for confidentiality of **MS's** identity IMSI.

This protocol achieves three goals as bellow: (a) **MS** and **VLR** achieve **unilateral authentication**. (b) **HLR** distributes a new session key K_c for **VLR** and **MS** to communicate. (c) In order to prevent the MS's true identity, **VLR** assigns an Temporary Mobile Subscriber Identity (TMSI) to **MS** in the current run of protocol that prevent the intruder to get the **MS'** true identity.

Although the GSM authentication protocol can perform some security requirement for secure communication, but it have some weakness.

(1) When a the **User** wants to access a service of the Network, he must transmit MS' s true identity on the air interface. This might lead to the **User** expose its true identity to attacks and be eavesdropped, and thus it' s not secure.

(2) If the one of insiders of **VLR** get K_c, RAND and SRES, it may be to embezzle impersonate the **User** to communication with the **VLR**.

(3) **MS**, **VLR** and **HLR** do not mutual authenticate each other.

(4) The cipher key Kc and authentication data are transmitted clearly between and within networks.

(5) The data integrity is not provided.

(6) If the secret key K_i were broken, the attacker can replay RAND to impersonate **VLR** to communicate with the **User**.

In the above, the security weakness will be enhanced in our new authentication protocols.

2.2.2 UMTS Authentication Protocol

Because the UMTS is building on the security of second-generation mobile system, therefore we will introduce the authentication protocol of the GSM mobile system and point out the weakness of the protocol [25].

In the following, we will introduce the authentication protocol of the UMTS. There are three authentication protocol schemes based on the results of the European ASPeCT (Advanced Security for Personal Communication Technologies) Project to be introduced [10] [29].

The three authentication protocol schemes are listed as follows:

(1) A Challenge/Response mechanism using symmetric key techniques (Royal Holloway College,London),

(2) A public key based mechanism (Siemens),

(3) A public key based mechanism (KPN).

Siemens defines three authentication protocol schemes, which are called A, B, and C, respectively.

The Protocol A

This protocol allows authentic copies of public keys of the **User** and the **Network Operator,** which are already available at the **Network Operator** and the **User,** respectively, and the public keys are not exchanged in the course of the protocol. The features of the protocol are listed as follows:

(1) Mutual authentication between the **User** and the **Network operator**.

(2) Establishment of a new session key Ks, which is a mutual key authentication shared between the **User** and the **Network Operator**. Mutual key freshness assurance.

(3) Mutual key confirmation of the **User** and the **Network operator**.

(4) The **User's** data sent by the **User** to the **Network Operator**, Non-repudiation achieved.

(5) The **User**' s identity IMUI confidentiality over the air interface.

Description of the protocol

The message flow consists of three messages exchanged between the **User** and the **Network Operator**. The messages are indicated in the **Figure 2.2** with M1, M2 and M3.

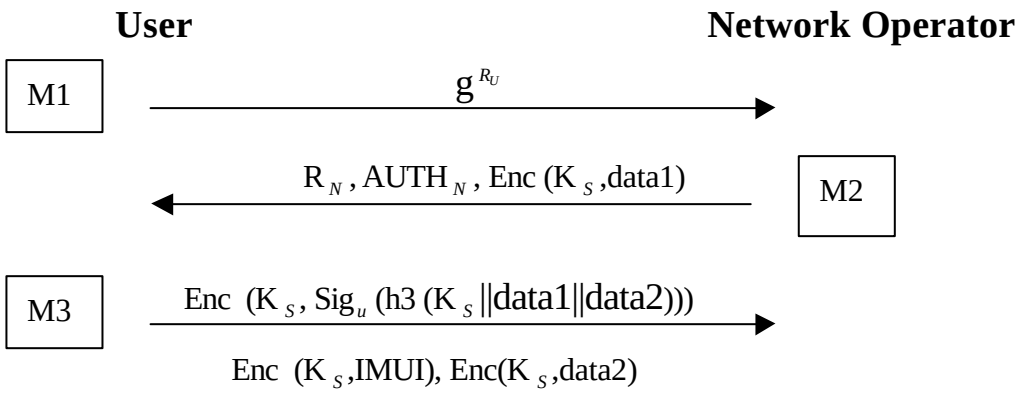

Figure 2.2. Siemens, Protocol A

Message M1:

The **User** generates a random number R_U and calculates a **Challenge** g^{R_U} send to the **Network operator**. When the **Network operator** receives this message, he will calculate the following entries:

– $(g^{R_U})^S$,

– the session key K_S = h1 $((g^{R_U})^S \| R_N)$,

– $AUTH_N$ = h2 (K_S).

Message M2:

The **Network operator** generates a random number R_N and $AUTH_N$, which are the challenge Enc (K_S, data1) and the response to the **User,** respectively. He then sends R_N, $AUTH_N$ and Enc (K_S, data1) to the **User** as the **User** receive these messages, he will calculate the following entries:

– $(g^S)^{R_U}$,

–Session key K_S = h1 $((g^S)^{R_U} \| R_N)$,

– $AUTH_N$ = h2 (K_S),

– Enc (K_S ,Sig_u (h3 (K_S||data1||data2))),

– Enc (K_S,IMUI),

– Enc (K_S,data2).

The **User** compares the received $AUTH_N$ with the one calculated by the **Network operator**.

Message M3:

The **User** sends Enc (K_S, Sig_u (h3 (K_S||data1||data2))), Enc (K_S,IMUI) and Enc (K_S,data2) to the **Network operator**.

The **Network Operator** does the following processes:

-Decrypts every part in the messaged, (K_S,Sig_u (h3 (K_S||data1||data2))), with decryption algorithm Dec and session key K_S.

–Learns the IMUI and knows which public key (PK_U) he has to retrieve from his database in order to verify the signature.

– Knows K_S, data1 and data2 and calculates h3 (K_S||data1||data2).

– Retrieves h3 (K_S||data1||data2) from Sig_u (h3 (K_S||data1||data2)) with verification algorithm Ver_u and key (PK_U). Then, the **Network Operator** compares the two values.

The Protocol B

This protocol is executed between the **User** and the **Network Operator**.

If a valid **User's** certificate based on the **User** public verification key PK_U is available at the **User** and not available at the **Network Operator**. Besides, if a valid **NO's** certificate is available at the **Network Operator** and is based on the **Network Operator** public key agreement key g^s, it would not be available at the **User**. The features of the protocol are listed as follows:

(1) Mutual authentication between the **User** and the **Network operator**.

(2) Establishment of a new session key Ks, which is a mutual key authentication shared between the **User** and the **Network Operator**. Mutual key freshness assurance.

(3) Mutual key confirmation of the **User** and the **Network operator**.

(4) The **User's** data sent by the **User** to the **Network Operator**, Non-repudiation achieved.

(5) The **User's** identity IMUI confidentiality over the air interface.

(6) The certified public keys are exchanged between the **User** and the **Network Operator**.

Description Of The Protocol

The message flow consists of three messages exchanged between the **User** and the **Network Operator**. The messages are indicated in the **Figure 2.3** with M1, M2 and M3. The difference with the protocol A is that the **User** does not know the public key of the **Network Operator** and the **Network Operator** does not know the public key of the **User**. Therefore, the **User** will include in the first message (M1) in which the

identification of the certification authority of which the **Network Operator** can verify signatures (id_{ca}). The **Network Operator** will include in the second message (M2) in which his certificate signed by the corresponding certification authority (CA). The **User** can verify this certificate (Cert N) and retrieves the public key agreement key g^S of the **Network Operator**, which is used for calculation of $(g^S)^{R_U}$. In the third message (M3), the certificate of the **User** (Cert U) is encrypted (Enc (K_S,Cert U)) replace of the IMUI. After receiving message M3, the **Network Operator** retrieves the public key of the **User** (PK_U) from the **User's** certificate and uses it for the other calculations.

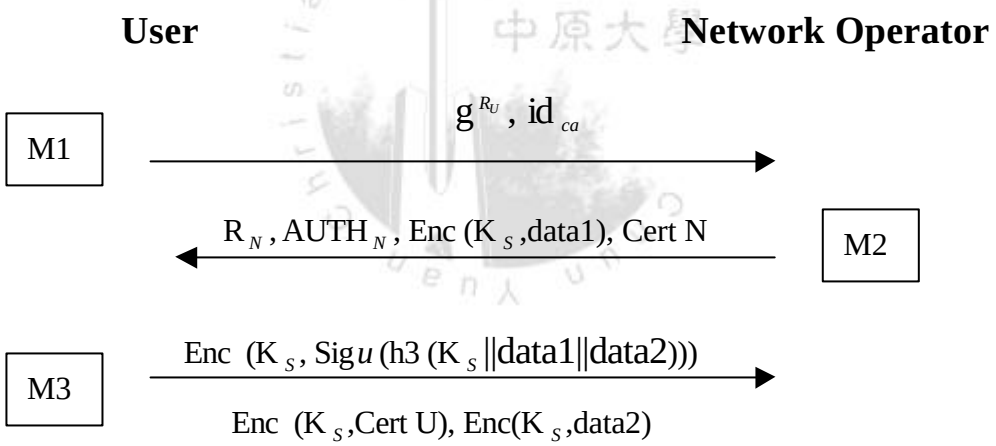

Figure 2.3. Siemens, Protocol B

The Protocol C

In this protocol , it is assumed that there is no authentic copy of the public key of the **User** available at the **Network Operator** and no authentic copy of the public key of the **Network Operator** available at the **User**, respectively.

Description Of The Protocol

The message flow consists of five messages exchanged among the **User**, the **Network Operator**, and a **Certificate Server** trusted by the **User**. The messages are indicated in the **Figure 2.4** with M1, M2, M3, M4, and M5.

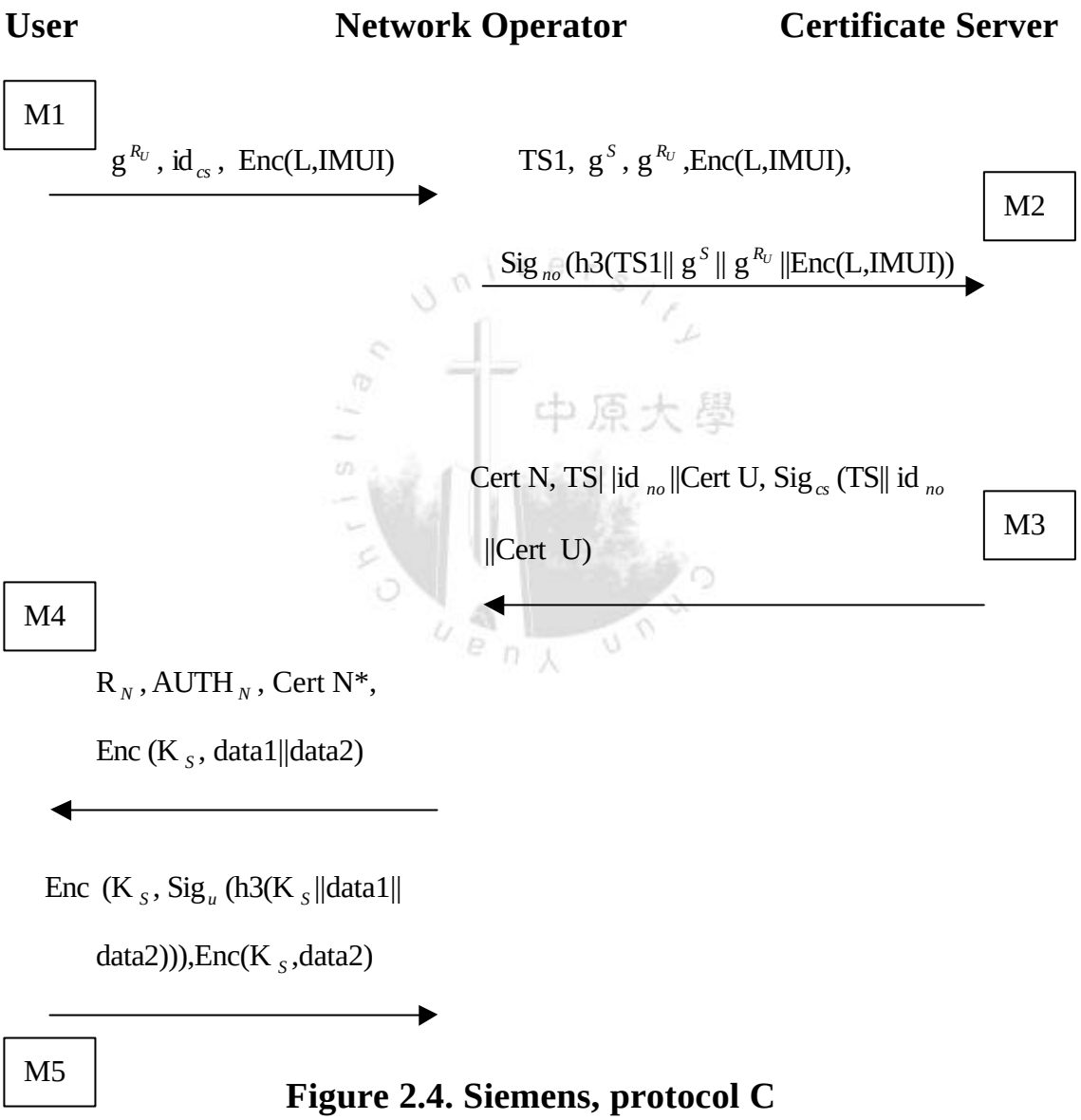

Figure 2.4. Siemens, protocol C

The **Certificate Server** (**CS**) can access a certificate, which is based on the public key of the **User** and is issued by a **Certification Authority**

(**CA**). **CS** may be identical with the **Service Provider** of the **User**. The flow of the messages exchanged between the **User** and the **Network Operator** is identical to that in protocols A and B. Over the air interface, the protocol itself is also very similar to protocols A and B. The major difference is a certified public key of the **Network Operator** distributed from the **Network Operator** to the **User**, but no certified public key is distributed from the **User** to the **Network Operator**.

There is a two-pass exchange of messages between the **Network Operator** and the **Certificate Server** in which **Certificate Server** distributes public keys of the **Network Operator** and the **User** to the **Network Operator**, which are signed by **CS**.

Message 1:

The **User** generates a random number R_U and calculates a **Challenge** g^{R_U}, L, and uses the secret key L to encrypt the IMUI of the **User**. Then, the **User** sends g^{R_U}, id_{cs} and Enc (L,IMUI) to the **Network operator**.

The **User** calculates the following entries:

– g^{R_U}

– $L = (g^u)^{R_U}$

– Enc (L,IMUI)

id_{cs} is the identification of the **Certificate Server** and the **User** can verify signatures. The **Network Operator** retrieves a (possibly new) public key g^S from storage and creates a time-stamp TS1. In the following steps, the **Network Operator** based on the new key g^S obtains a certificate from the **Certificate Server**. The **Network Operator**

calculates a signature on TS1 || g^{S} || g^{R_U} || Enc (L,IMUI) with the hash function h3, signature algorithm Sig_{no} and key SK_NO

Message M2:

The **Network Operator** sends TS1, g^{S}, g^{R_U}, Enc(L , IMUI) , Sig_{no}(h3 (TS1 || g^{S} || g^{R_U} ||Enc (L,IMUI))) to the **Certificate Server**. While the **Certificate Server** receives these messages, he calculates h3 (TS1 || g^{S} || g^{R_U} || Enc (L , IMUI)) and verifies the received signature with verification algorithm Ver_{no} and public key PK_NO. Afterwards, he checks the Time Stamp TS1 and calculates L:

– L = $(g^{R_U})^{u}$

– Using the decryption algorithm Dec and key L to decrypts Enc (L , IMUI).

– Retrieves Cert U associated with the obtained IMUI from its database.

– Checks the (eventually new) key g^{S} of the **Network Operator** and the certificate Cert U against revocation lists.

– Creates the credentials = g^{R_U} || g^{S} || id_{no} || data3 and calculates a certificate on the **Network Operator**'s public key agreement key i.e., Cert N which is a signature on the credentials, Cert N =credentials, Sig_{cs} (h3 (credentials)). The data3 is an optional field transmitted to the **User** in an authentic way.

– Creates a new time stamp TS and calculates a signature on TS || id_{no} || Cert U.

Message M3 :

The **Certificate Server** sends Cert N, TS || id_{no} || Cert U, Sig_{cs} (TS || id_{no} || Cert U) to the **Network Operator**.

When the **Network Operator** receives these messages, he verifies the signature on TS || id_{no} || Cert U and the Cert N with verification algorithm Ver_{cs} and key PK_CS. Afterwards, the **Network Operator** calculates:

– A shortened Cert N named Cert N* = g^{S} || Sig_{cs} (h3 (credentials)).

– $(g^{R_U})^{S}$

– The session key K_S = h1 ($(g^{R_U})^{S}$ || R_N)

– AUTH N = h2 (K_S)

– Enc (K_S, data1 || data3) encrypted with algorithm Enc and key K_S

data1 is an optional data field sent from the **Network Operator** to the **User** in an authentic way.

Message M4 :

The **Network Operator** sends R_N, $AUTH_N$, Cert N* and Enc(K_S,data1 || data3) to the **User**. The **User** reconstructs the credentials = g^{R_U} || g^{S} || id_{no} || data3 and verifies the signature on Cert N (which is Sig_{cs} (h3 (credentials)) and is part of Cert N*) with verification algorithm Ver_{cs} and key PK_CS.

The **User** calculates the following entries:

– $(g^{S})^{R_U}$

– The session key K_S = h1 ((g^S) ^{R_U} || R_N)

– $AUTH_N$ = h2 (K_S)

– data1 || data3 = decryption of Enc(K_S,data1 || data3) with decryption algorithm Dec and key K_S

– Enc (K_S, Sig_u (h3(K_S||data1||data2)))

– Enc (K_S,data2)

The **User** compares the received $AUTH_N$ with the calculated one from the **Network operator**.

Message M5 :

The **User** sends Enc (K_S, Sig_u (h3 (K_S||data1||data2))), Enc(K_S,data2) to the **Network Operator**. The **Network Operator** receives these messages and calculates the following entries:

– Decrypts every part of the message with decryption algorithm Dec and session key K_S

– Knows K_S, data1 and data2 and calculates h3 (K_S||data1||data2)

– Retrieves h3 (K_S||data1||data2) from Sig_u (h3 (K_S||data1||data2)) with verification algorithm Ver_u and key PK_U. Afterwards, the **Network Operator** compares these two values.

2.3 Security Threats and Requirements of UMTS

In general, many telecommunication service and application will not be standardized, because it is difficult to predict their exact nature. Therefore, ETSI, which is in the European to draw up a set of specifications, is concerned with Security Threats and Requirement of UMTS [30](see Appendix B). In this specification, the threat analysis performed relies to a large extent on previous experiences with 2G systems, in particular GSM, and takes into account known problems from that area. The security requirements listed in this specification shall be used as input for the choice of security features and the design of the authentication protocol. In this thesis, we will follow this specification (Appendix B) and the general objectives for 3G security features (see Appendix C) to design our new authentication protocols.

2.4 **Abbreviations**

This section lists the symbols and notations used in the Siemens and our proposes protocols.

GSM: **G**lobal **S**ystem for **M**obile Communications.

HLR: **H**ome **L**ocation **R**egister.

IMUI: **I**nternational **M**obile **U**ser **I**dentity.

SRES: **S**igned **Res**ponse.

VLR: **V**isitor **L**ocation **R**egister.

‖: concatenation.

$\mathbf{AUTH}_N$: The Value is used to authenticate the **Network Operator** to the **User**, mostly this will be a challenge response value.

AUTH$_U$: The Value is used to authenticate the user to the **Network Operator**, mostly this will be a challenge response value.

CA: **C**ertification **A**uthority.

Cert N: It is a valid certificate, issued by a Certification Authority CA, on the public key of the asymmetric signature system of N, available at N.

Cert U: It is a valid certificate, issued by a Certification Authority CA, on the public key of the asymmetric signature system of U, available at U.

data1, data2, data3: They are optional data fields.

Dec: A decryption algorithm, corresponding with the encryption algorithm Enc (see below).

Enc: A symmetric encryption algorithm. Enc (K, data) means data encrypted with encryption algorithm Enc and key K.

g: It is a generator g, known by UIM/terminal, **Network Operator**, and **Service Provider**. g is a generator of a finite group G, e.g., the multiplicative group of a finite field or a subgroup of an elliptic curve, in which the Discrete Logarithm Problem is hard.

g ^{S} : It is a public key agreement key of the **Network Operator**.

g ^{U} : It is a public key agreement key of the **Certificate Server**.

h1: one-way function.

h2: hash function.

h3: hash function.

id$_{ca}$: It is the identity of the Certification Authority.

id$_{cs}$: It is the identity of the Certificate Server.

id_{no}: It is the identity of the **Network Operator**.

Ks: It is the secret session key shared between **User** and **Network Operator**.

L: The length of session key Ks.

NO: **Network operator**.

R_N: It is a Random challenge, generated by the **Network Operator**.

R_U: It is a Random challenge, generated by the **User**.

S: It is a secret key agreement key of the **Network Operator**.

Sig_{cs}: A secret signature transformation owned by the **Certificate Server**.

Sig_{no}: A secret signature transformation owned by the **Network Operator**.

Sig_U: A secret signature transformation owned by the **User**.

Chapter 3 Three Proposed Schemes of Authentication Protocol

In this chapter, we use the representation of message flow proposed by [28] to reconstruct three authentication protocols of proposed by the Siemens and propose three new authentication protocol schemes for the third generation mobile communication systems.

3.1 Reconstruction of Three Authentication Protocols Using another Representation of Message Flow

In general, **Challenge/Response** and **Time-Stamp** are usually used to achieve authentication manner for the authentication protocols (introduced in section 2.1).

In the mobile communication environment, the **Challenge/Response** manner is easier to implementation than Time-stamp, because the Time-Stamp manner has a problem of synchronization. Therefore, the **Challenge/Response** is a good manner to design an authentication protocol for the mobile communication.

In the authentication protocol, the designer usually sends the all messages included in each transmission step. However it is difficult for us to understand these messages and their relationship explicitly. Therefore, we use another representation of message flow proposed by [28] to reconstruct the protocol in order to assist us to understand these messages and relationship in each transmission step. The protocols A, B and C represented by this message flowchart are shown in the **Figure 3.1**, **Figure 3.2**, and **Figure 3.3,** respectively.

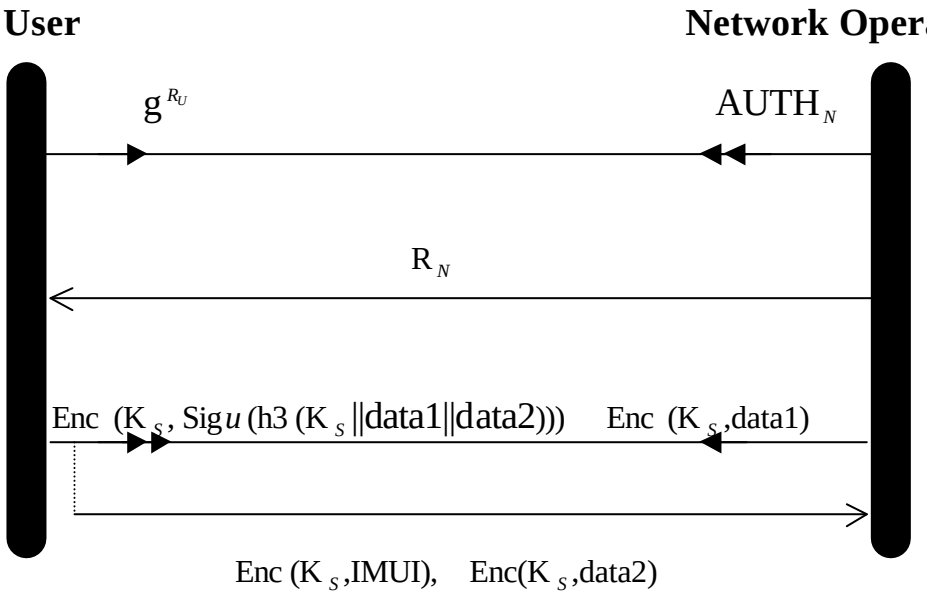

Figure 3.1. Another representation of message flow for the Protocol A

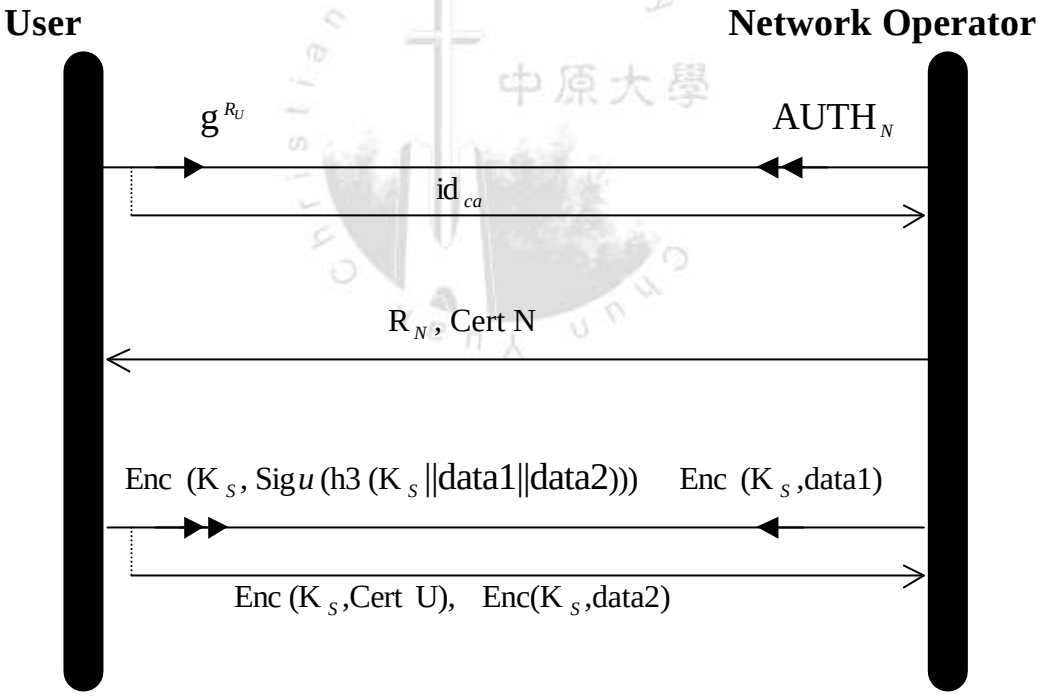

Figure 3.2. Another representation of message flow for the Protocol B

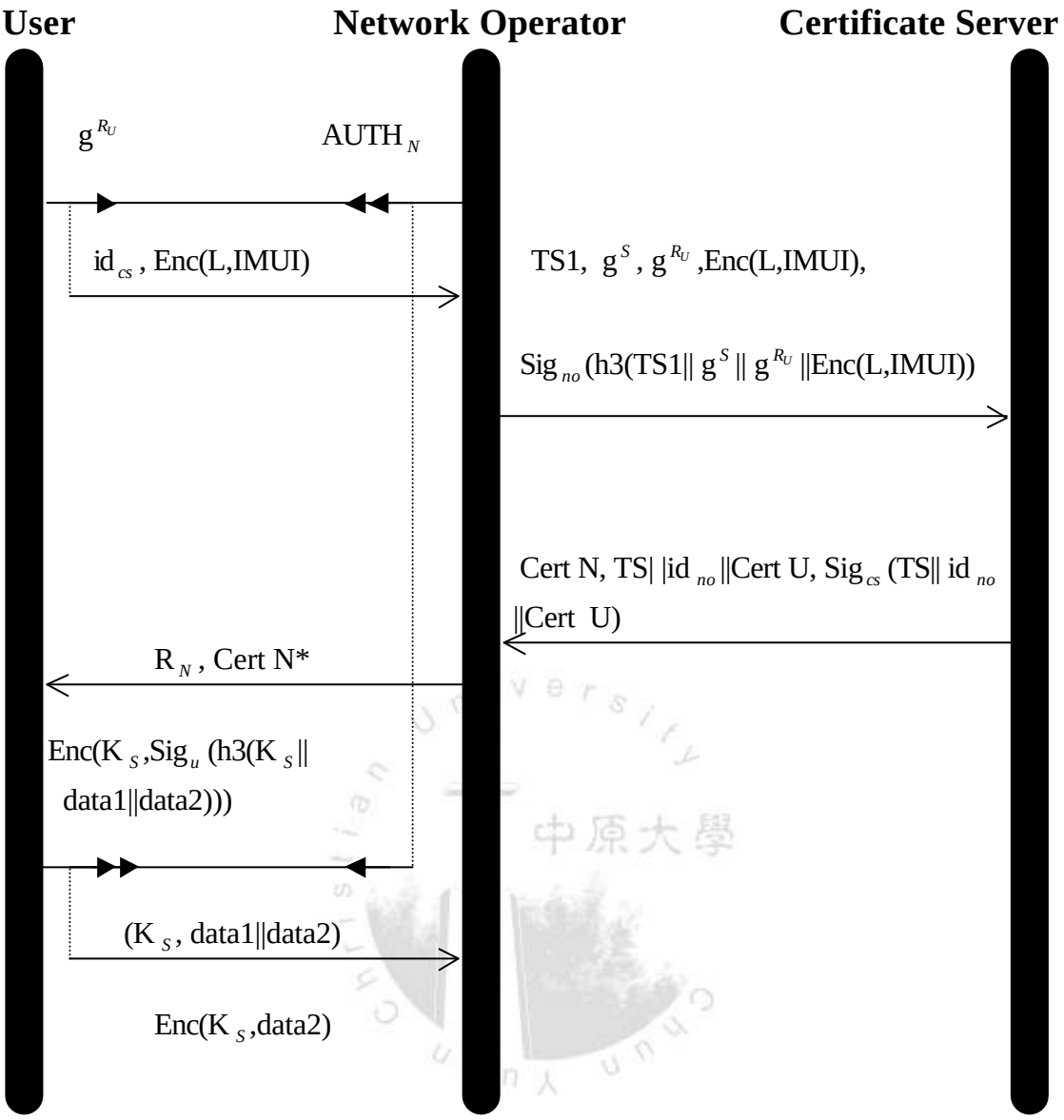

Figure 3.3. Another representation of message flow for the Protocol C

3.2 The First Scheme of Authentication Protocol

Main Idea

In symmetric cryptosystem, between encipher and decipher a secret key is shared. The advantage of secret key is that it provides fast speed operations of the encryption and decryption. However, there are some functions cannot be achieved in symmetric cryptosystem. There involves the key management problem and the queried security. Therefore, Diffie and Hellman propose a concept of public key based cryptosystem in 1976 [31]. The advantage of the public key is that it is able to solve these problems, which cannot be achieved by secret key cryptosystem. Therefore, the public key cryptosystem research has become a main stream of the modern cryptography theory.

According to the reasons described above, we decide to employ a public key encryption and decryption tools to design a authentication protocol. The three authentication protocols proposed by the Siemens [29] are used with the signature method. Therefore, we try to use the public key cryptosystem approach to achieve the goals of authentication protocol such as authentication data, session key generation, secret data and mutual authentication, and so on. According to the security requirements defined in document (ETSI TS 21.133, see Appendix C), there are some goals, which have to be achieved before the subscriber is permitted to use the service from the **Network Operator**. The main advantages of our protocol are twofold (1) to solve a key management problem (2) to provide higher operation speed compared with the protocols proposed by Siemens.

The First Protocol

The first protocol is applied to achieve the goals such as the mutual authentication of the **User** and the **Network Operator** and the establishment of shared session key K_S between them.

Goals

The goals of the first scheme are described as follows:

(G1) Mutual explicit authentication between the **User** and the **Network Operator**.

(G2) Agreement between the **User** and the **Network Operator** on shared session key K_S with mutual explicit key authentication.

(G3) Mutual key confirmation of the **User** and the **Network operator**.

(G4) Mutual assurance of key freshness

(G5) The confidentiality of the **User's** identity over the air-interface.

(G6) The confidentiality of the **User's** identity to the **Network Operator**.

Prerequisites On Mechanism

Initially, the **Network Operator** identity is assumed to be known by the **User.** In addition,

(1) the **Network Operator** has a secret key SK_NO and a public key of the **User**- K_U;

(2) the **User** has a secret key SK_U and a public key of the **Network Operator**- K_N.

Description Of The Protocol

At first, we consider the first protocol that consists of three exchanged messages between the **User** and the **Network Operator**. The **Service Provider** does not involve this scheme. The messages flows are indicated in the **Figure 3.4** with M1, M2 and M3. In this protocol, the **User** has already registered with the **Network Operator** where it is roaming. The **User** and the **Network Operator** have already shared some information described above.

The First Protocol

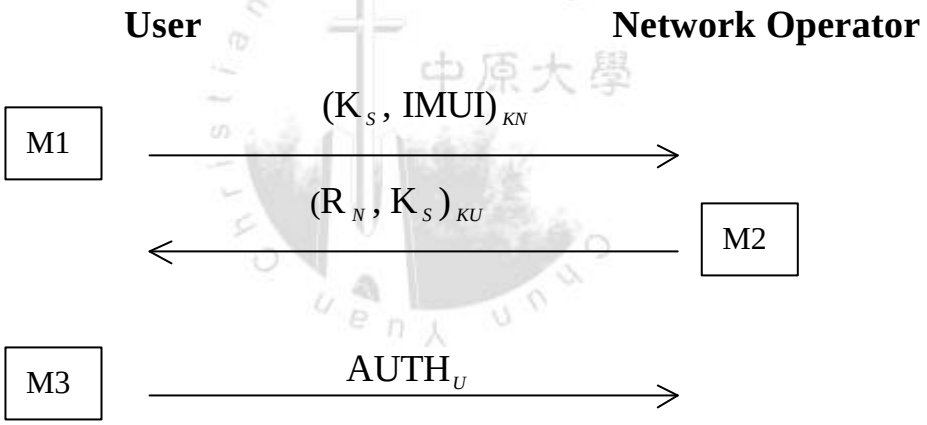

Figure 3.4. The First Protocol

The notations in **Figure 3.4** are defined as follows:

- U: **User**
- NO: **Network Operator**.
- CA: **Certification Authority**.
- CS: **Certificate Server**.

- $K_X \equiv$ X's public key, where X= N, U, CS.

- $K_S \equiv$ The session key is shard between the **User** and the **Network Operator**

- IMUI: International Mobile **User** Identity.

- data1||data2 : Concatenation data1 and data2 alongside the notation ||.

- $ID_X \equiv$ X's identity, where X=CA, CS.

- $R_X \equiv$ A random number generated by X= U, N.

- $Auth_{AB} \equiv$ A authentication function between A and B.

- $AUTH_U = (R_N)_{Ks}$.

The Value of the $(R_N, K_S)_{KU}$ used to authenticate the **User** to the **Network Operator**, generally this will be a challenge response value. The Value of the $AUTH_U$ is used to authenticate the **Network Operator** to the **User**, generally this will be a challenge response value.

Instead of representation of the message flow illustrated in **Figure 3.4**, we use the representation of message flow proposed by [28] to reconstruct the first protocol as shown in **Figure 3.5**.

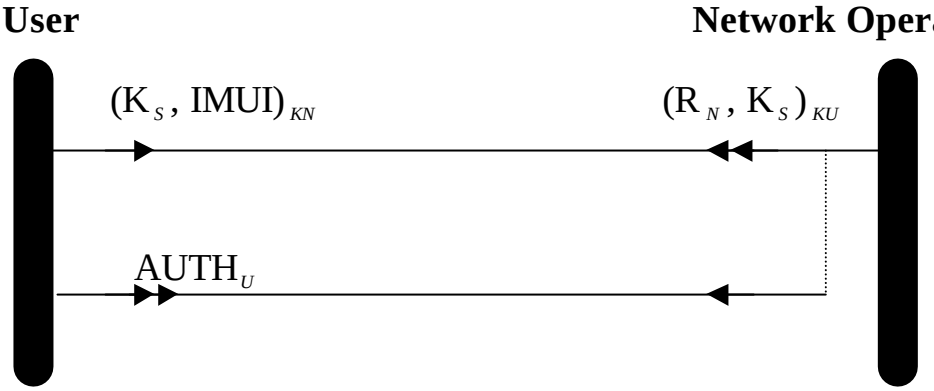

Figure 3.5. New message flow for the First protocol

Next, we explain the message exchanged involved in the protocol of **Figure 3.4** in details.

Message M1:

The **User** sends $(K_S, IMUI)_{KN}$ to the **Network Operator**, where $(K_S, IMUI)_{KN}$ is a challenge message for a registration request. When the **Network Operator** receives the message M1, he decrypts $(K_S, IMUI)_{KN}$ based on his secret key to gets IMUI and K_S. The **Network Operator** will find the public key of the **User** to encrypt the data, afterward. At the same time, the **Network Operator** generates a random number R_N and encrypts R_N as $(R_N)_{KU}$, which is a challenge and response number.

Message M2:

The **Network Operator** sends $(R_N, K_S)_{KU}$ to the **User**. When the **User** receives the Message M2, he decrypts $(R_N, K_S)_{KU}$ based on his secret key. When **User** gets R_N and K_S, he checks the session key K_S from the **Network Operator** with the sends one. If the calculated value is correct, the goal of the authentication of the **User** to the **Network Operator** has been achieved. Furthermore, the **User** sends the $AUTH_U$, which is the response to the **Network Operator**.

Message M3:

The **User** sends $AUTH_U$ to the **Network Operator**. When the **Network Operator** receives the Message M3, he checks the $AUTH_U$ and compares it from the **User** with the sends one. If the calculated value is correct, the goal of the authentication of the **Network Operator** to the **User** has been achieved.

Achieved Goals

The achieved goals of the first protocol are described as follows.

Entity authentication of the **User** to the **Network Operator**:

By verifying $(R_N, K_S)_{KU}$, the **User** knows that K_S is send by him. Therefore, the **User** can authenticate **NO's** identity.

Entity authentication of the **Network Operator** to the **User**:

By verifying $AUTH_U$ the **User** knows that R_N is based on Network Operator. Therefore, **Network Operator** can authenticate the **User's** identity.

Assurance to the **User** that the Session key is fresh:

The session key is derived from the **User**.

Assurance to the **Network Operator** that the Session key is fresh:

The session key is derived from the random value R_N.

Session Key authentication of the **User** to the **Network operator**:

It is because that the value $AUTH_U$ is included in the Message M3.

Session Key confirmation of the **Network Operator** to the **User**:

It is because that the value $(K_S, R_N)_{KU}$ is included in the Message

M2.

Security Analysis

In the following, in order to ensure that the protocol is secure, we shall analyze and discuss the attack methods [35-42].

Attacks 1:Replay attacks [33]

In this case, to prevent replay attacks, a message in the protocol should contain some "freshness" properties. In the message M1 and M2, the **User** and the **Network Operator** generates a session key K_S and the random number R_N respectively as the fresh messages. In the message M2, the **User** can check K_S according to $(R_N, K_S)_{KU}$ if the message is fresh in this round. In the message M3, the **Network Operator** can verify the $AUTH_U$ that knows the freshness property. Besides, the $(K_S, R_N)_{KU}$ represents the freshness property because it is encrypted by the **User**'s public key such that only the **User** can decrypt it. Similarly, $(R_N, K_S)_{KU}$ represents the freshness property since the session key encrypts it, such that only the **Network Operator** can decrypt it. Hence, the replay attacks are infeasible.

Attack 2: Parallel session attacks [34]

Since the messages M1, M2 and M3 fit the asymmetric condition; the parallel session attacks are infeasible.

Attack 3: Guessing Attacks [33]

The authentication with password is widely used by many security systems. However, password is vulnerable under the dictionary attack by which an attacker can guess the password successfully. Public key provides a means for preventing the guessing attack. Since, we uses the public key to encrypt the message, the guessing attacks are infeasible.

3.3 The Second Scheme of Authentication Protocol

Main idea

The main idea of the second authentication protocol is the same with the First protocol. The second protocol is applied to achieve the goals, such as the mutual authentication of the **User** and the **Network Operator** and establishment of shared session key K_S between them and use a valid certification.

Goals

The goals of the second scheme are described as follows:

(G1) Mutual explicit authentication between the **User** and the **Network Operator**.

(G2) Agreement between the **User** and the **Network Operator** on shared session key K_S with mutual explicit key authentication.

(G3) Mutual key confirmation of the **User** and the **Network operator**.

(G4) Mutual assurance of key freshness

(G5) The confidentiality of the **User's** identity over the air-interface.

(G6) The confidentiality of the **User's** identity to the **Network Operator**.

(G7) Exchange of certified public keys between the **User** and the **Network Operator**.

Prerequisites On Mechanism

The prerequisites of this protocol are the same as for the first protocol except that:

(1) the **User** has no authentic copy of the public key K_N of the **Network Operator**.

(2) The **Network Operator** has no authentic copy of the public verification key K_U of the **User**.

(3) There is a valid certificate Cert U, issued by a Certification Authority **CA**, on the public key K_U of the **User**, available at the **User**.

(4) There is a valid certificate Cert N, issued by a Certification Authority **CA** on the public key K_N of the **Network Operator**, available at the **Network Operator**.

(5)The **User** and the **Network Operator** possess the public key necessary to verify certificates issued by CA (PK_CA).

Description Of The Protocol

At first, we consider the second protocol that consists of four exchanged messages between the **User** and the **Network Operator**. The messages flows are indicated in the **Figure 3.6** with M1, M2, M3, and M4. The difference with first protocol is that the **User** does not know the public key of the **Network Operator** and the **Network Operator** does not know the public key of the **User**.

The Second Protocol

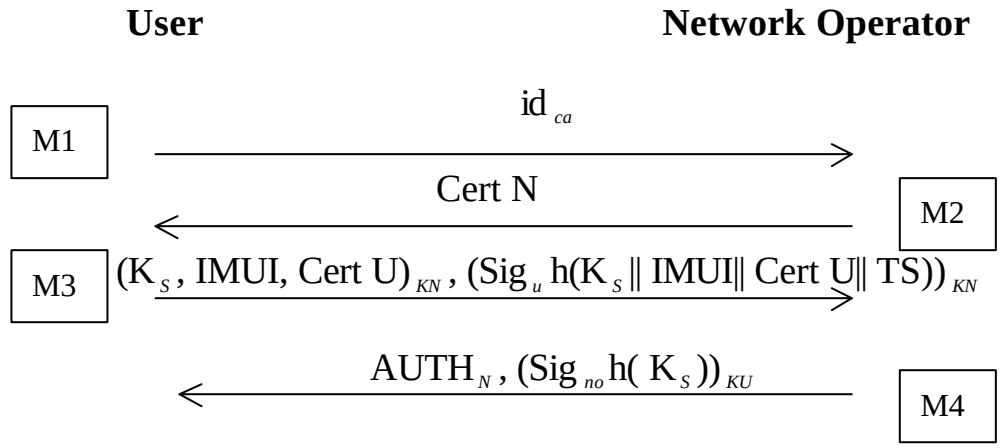

Figure 3.6 The Second Authentication Protocol

The notations in **Figure 3.6** are defined as follows:

- id_{ca} is an identity of the Certification Authority.

- Cert N a valid certificate, issued by a Certification Authority **CA**, on the public key of the asymmetric signature system of the **Network Operator**, available at the **Network Operator**.

-Cert U a valid certificate, issued by a Certification Authority **CA**, on the public key of the asymmetric signature system of the **User**, available at the **User**.

-Sig_{no} is a secret signature transformation owned by the **Network Operator.**

-Sig_u is a secret signature transformation owned by the **User**.

-TS is a time stamp.

- $AUTH_N = (K_S)_{KU}$

The Value of the $AUTH_N$ is used to authenticate the **User** to the **Network Operator**, generally this will be a challenge response value.

Instead of representation of the message flow illustrated in **Figure 3.6**, we use new representation of message flow [28] to reconstruct the Second protocol as shown in **Figure 3.7**.

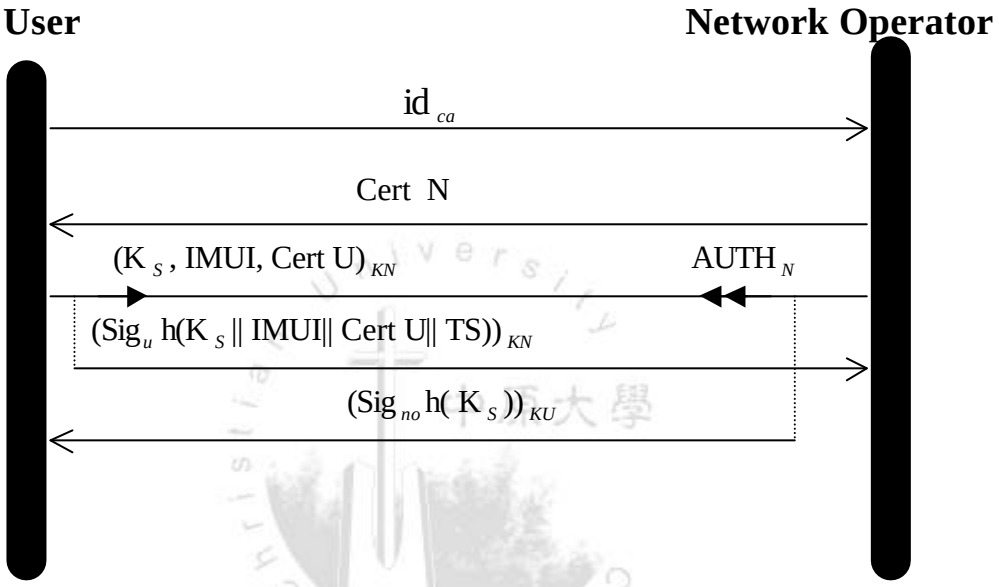

Figure 3.7. New message flow for the Second protocol

Next, we explain the message exchanged involved in the protocol of **Figure 3.6** in details.

Message M1:

The **User** sends id_{ca}, the identification of the **Certification Authority**, to the **Network Operator**, that the **Network Operator** can verify the signatures. When the **Network Operator** receives this message, he will send his certificate signed by the corresponding **Certification Authority** (**CA**) to uses in Message M2.

Message M2:

Network Operator sends Cert N to **User.** The **User** can verify this certificate and retrieves the public key agreement key K_N of the **Network Operator**.

Message M3:

The **User** sends $(K_S, \text{IMUI, Cert U})_{KN}$ and $(\text{Sig}_u h(K_S \| \text{IMUI} \| \text{Cert U} \| \text{TS}))_{KN}$ to the **Network Operator**, where $(K_S, \text{IMUI, Cert U})_{KN}$ is a challenge message. Cert U, IMUI and TS are based on the public key K_N of the **Network Operator**. The **User** generates K_S, which is a session key between the **User** and the **Network Operator**. When the **Network Operator** receives these messages, he decrypts $(K_S, \text{IMUI, Cert U})$ as $(K_S, \text{IMUI, Cert U})_{KN}$ based on his secret key and gets IMUI, K_S and Cert U. The **Network Operator** retrieves the public key of the **User** K_U from the **User's** certificate, Cert U, and checks the signature. When the **Network Operator** gets IMUI, he verifies the identification of the **User**.

Message M4:

The **Network Operator** sends AUTH_N and $(\text{Sig}_{no} h(K_S))_{KU}$ to the **User**. **When** the **User** gets AUTH_N, he compares the received AUTH_U from the **Network Operator** with the sends one. If the calculated value is correct, the goal of the authentication of the **User** to the **Network Operator** has been achieved. The **User** retrieves the public key of the

Network Operator K_N from the **Network Operator**'s certificate, Cert N, and checks the signature.

Achieved Goals

The achieved goals of the second protocol are described as follows. The prerequisites of this protocol are the same as for the first protocol except that:

-Exchange of certificates: id_{ca} is sent in Message M1 to indicate **Network Operator** which certificates can be verified by the **User**. The **Network Operator** sends a certificate, Cert N, to the **User** in Message M2 and the **User** sends a certificate, Cert U, to the **User** in Message M3.

-Non-repudiation of data sent by the **User**: The **User** sends $(Sig_u h(K_S \| IMUI \| Cert U \| TS))_{KN}$ to the **Network Operator**.

-Non-repudiation of data sent by the **Network Operator**: The **Network Operator** sends $(Sig_{no} h(K_S))_{KU}$ to the **User**.

Security Analysis

In the following, in order to ensure that the protocol is secure, we shall analyze and discuss the attack methods [35-42].

Attacks 1: Replay attacks [33]

In this case, to prevent replay attacks, a message in the protocol should

contain some "freshness" properties. In the message M3, the **User** generates a session key K_S and the time stamp TS as the fresh messages. In the message M4, the **User** can check K_S according to $AUTH_N$ if the message is fresh in this round. Besides, the $AUTH_N$ represents the freshness property because it is encrypted by the **User's** public key such that only the **User** can decrypt it. Hence, the replay attacks are infeasible.

Attack 2: Parallel session attacks [34]

Since the messages M1, M2 and M3 fit the asymmetric condition; the parallel session attacks are infeasible.

Attack 3: Guessing Attacks [33]

The authentication with password is widely used by many security systems. However, password is vulnerable under the dictionary attack by which an attacker can guess the password successfully. Public key provides a means for preventing the guessing attack. Since, we uses the public key to encrypt the message, the guessing attacks are infeasible.

Attack 4: Man-in-the-Middle Attacks [33]

An attacker can use the man-in-the-middle attack to intervene between the **User** and the **Network Operator** and masquerade as one to communicate with another bidirectionally. Public key cryptosystem using certificate often provides a solution for preventing this attacks. Since, our scheme can prevent these attacks.

3.4 The Third Scheme of Authentication Protocol

Main idea

The main idea of the third authentication protocol is the same with the first protocol. **Certificate Server** applies the third protocol to achieve the goals such as the mutual authentication of the **User** and the **Network Operator**, the establishment of shared session key K_S between them and valid certification provided by the **Certificate Server** .

Goals

The goals of the third scheme are described as follows:

(G1)-(G6) are the same as those of the first protocol.

(G7) Distribution of public key K_U of the **User** certified by a **Certification Authority** (**CA**) from the **Certificate Server** (**CS**) to the **Network Operator**.

(G8) Distribution of the public key K_N of the **Network operator** certified by the **Certificate Server** from the **Network operator** to the **User**.

(G9) Assurance for the **Certificate Server** that the publics key it certifies is indeed the public key of the **Network operator**.

Prerequisites On Mechanism

The prerequisites of this protocol are the same as for the first protocol except that:

(1) The **User** has a public key the **Certificate Server**-K_C .

(2) The **Network Operator** has a public key the **Certificate Server**-K_C .

Description Of The Protocol

The third protocol is no authentic copy of the public key of the **User** available at the **Network Operator** and is no authentic copy of the public key of the **Network Operator** available at the **User**.

In the third protocol, there are five exchanged messages among the **User**, the **Network Operator** and the **Certificate Server**. The messages flows are indicated in the **Figure 3.8**. The **certificate server CS** has to access the certificate of the **User** issued by a **Certification Authority CA**.

The notations in **Figure 3.8** are defined as follows:

- id_{cs} is a identity of the **Certificate Server**.

- $K_S = h1(R_U \oplus R_N)$.

- $AUTH_N = h2(K_S)$.

- $AUTH_U = h3(K_S)$.

The Third Protocol

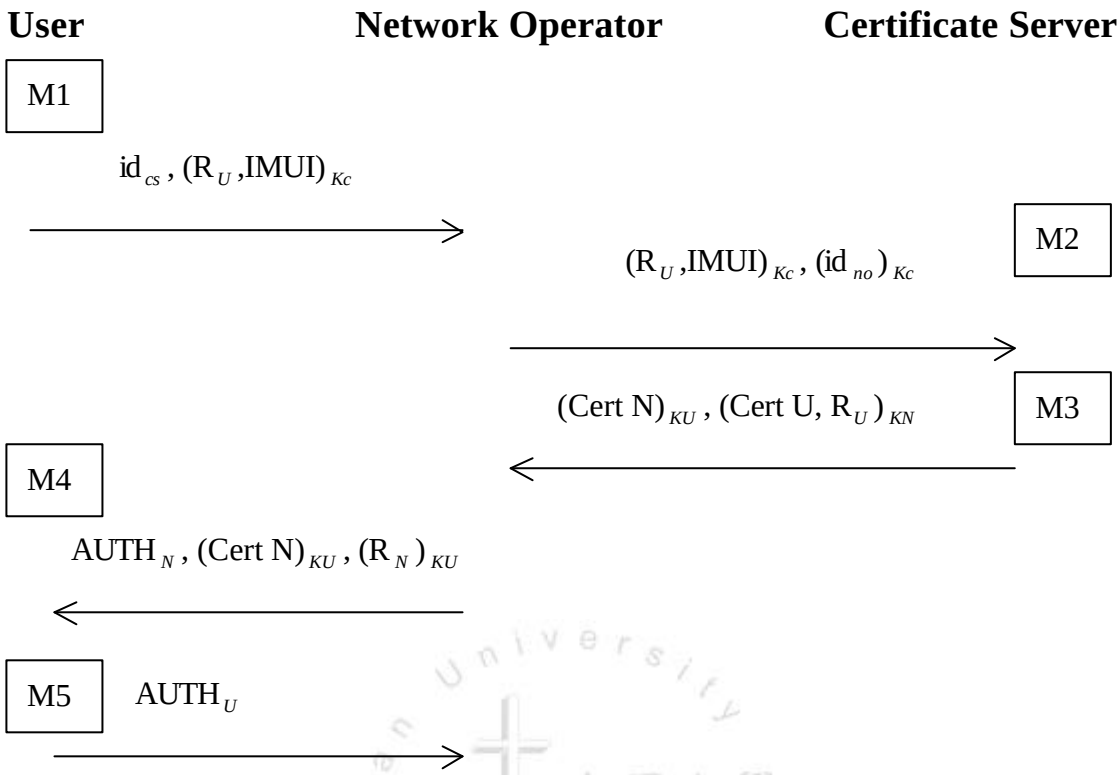

Figure 3.8. The Third Protocol

Instead of representation of the message flow illustrated in **Figure 3.8**, we use the representation of message flow proposed by [28] to reconstruct the third protocol as shown in **Figure 3.9**.

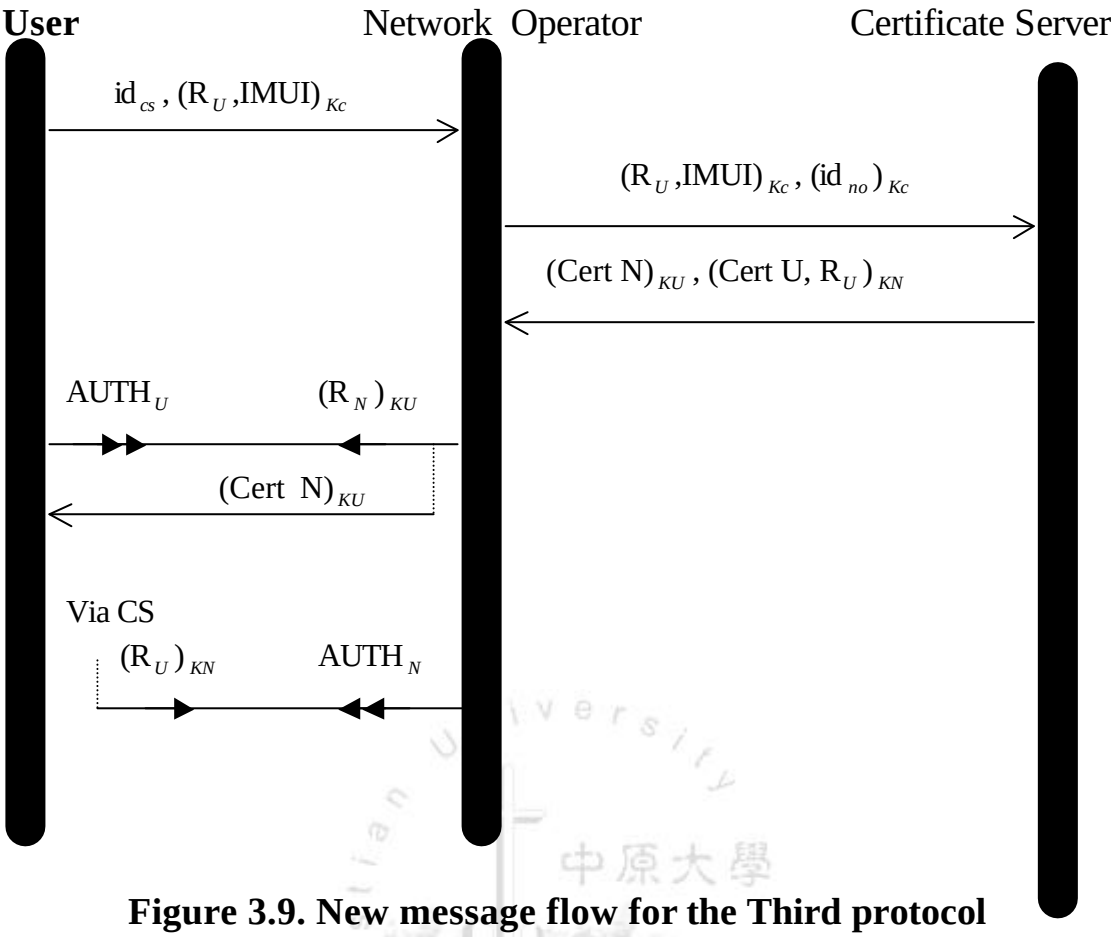

Figure 3.9. New message flow for the Third protocol

Next, we explain the message exchanged involved in the protocol of **Figure 3.8** in details.

Message M1:

User sends id_{cs} and $(R_U, IMUI)_{Kc}$ to the **Network Operator**. The id_{cs} is the identification of the **Certificate Server** that the **User** can verify signatures.

Message M2:

When the **Network Operator** receives these messages, it forwards the

message of $(R_U, IMUI)_{Kc}$ and uses the **Certificate Server's** public key K_C to encrypt his identity id_{no}, then sends these messages to the **Certificate Server**. The **Certificate Server** receives these messages, he decrypts the $(R_U, IMUI)_{Kc}$ and $(id_{no})_{Kc}$ based on his secret key K_C. The **Certificate Server** gets R_U, IMUI and id_{no}. It uses IMUI and id_{no} to access the database of the **Certificate Server** to obtain Cert U and Cert N, respectively.

Message 3:

The **Certificate Server** sends $(\text{Cert N})_{KU}$ and $(\text{Cert U}, R_U)_{KN}$ to the **Network Operator**. When the **Network Operator** receives these messages, he decrypts $(\text{Cert U}, R_U)_{KN}$ based on his secret key and gets Cert U, R_U. At the same time, the **Network Operator** generates a random number R_N, and calculates the session key K_S and $AUTH_N$

Message M4:

The **Network Operator** sends $AUTH_N$, $(\text{Cert N})_{KU}$, and $(R_N)_{KU}$ to the **User**. When the **User** receives these messages, he decrypts $(R_N)_{KU}$ and $(\text{Cert N})_{KU}$ based on his secret key and gets R_N, Cert N. Therefore, the **User** compares the received $AUTH_N$ from the **Network Operator** with the calculated one. If the calculated value is correct, the goal of the authentication of the **User** to the **Network Operator** has been achieved.

Furthermore, the **User** calculates the $AUTH_U$, which is response to the **Network Operator**.

Message M5:

The **User** sends $AUTH_U$ to the **Network Operator**. When the **Network Operator** receives these messages, he compares the received $AUTH_U$ from the **User** with the calculated one. If the calculated value is correct, the goal of the authentication of the **Network Operator** to the **User** has been achieved.

Achieved Goals

The achieved goals of the third protocol are described as follows. The same goals are achieved in the same way as for first protocol except for:

-Confidentiality of the **User** identity:

It is achieved by encrypting the **User** identity IMUI in the first message with public key K_C of the **Certificate Server**.

-Exchange of certificates:

id_{cs} is sent in message M1 to indicate to the **Certificate Server** which certificates can be verified by the **User**.

Security Analysis

In the following, in order to ensure that the protocol is secure, we shall analyze and discuss the attack methods [35-42].

Attacks 1: Replay attacks [33]

In this case, to prevent replay attacks, a message in the protocol should contain some "freshness" properties. In the message M1 and M4, the **User** and the **Network Operator** generates a session key R_U and the random number R_N, respectively, as the fresh message. In the message M4, the **User** can check K_S according to $AUTH_N$ if the message is fresh in this round. In the message M5, the **Network Operator** can verify the $AUTH_U$ that knows the freshness property. Besides, the random number R_N represents the freshness property because it is encrypted by the **User's** public key such that only the **User** can decrypt it. Similarly, the $(R_U)_{KN}$ represents the freshness property because it is encrypted by the **Network Operator**'s public key such that only the **Network Operator** can decrypt it. Hence, the replay attacks are infeasible.

Attack 2: Parallel session attacks [34]

Since the messages M1, M2, M3, M4, and M5 fit the asymmetric condition, the parallel session attacks are infeasible.

Attack 3: Guessing Attacks [33]

The authentication with password is widely used by many security systems. However, password is vulnerable under the dictionary attack by which an attacker can guess the password successfully. Public key provides a means for preventing the guessing attack. Since we use the public key to encrypt the message, the guessing attacks are infeasible.

Attack 4:Man-in-the-Middle Attacks [33]

An attacker can use the man-in-the-middle attack to intervene between the **User** and the **Network Operator** and masquerade as one to communicate with another bidirectionally. Public key cryptosystem using certificate often provides a solution for preventing this attacks. Since, our scheme can prevent these attacks.

3.5 Performance Analysis

In this case, we compare the performance of our protocols and Siemens protocols. Our protocols have the feature of transmission data size within communications less than the protocols proposed by Siemens. The comparisons are list in Table 1 and Table 2 as follows:

Table 3.1. Performance Evaluations

Performance evaluation	Siemens Bits	Our Proposed Bits	Performance h
Protocol A/Protocol 1	896 bits	640 bits	71.42%
Protocol B/Protocol 2	1280 bits	924 bits	72.18%
Protocol C/Protocol 3	2176 bits	1412 bits	64.88%

* The number of bits is reference by 3GPP [5].

Table 3.2. Comparison of Our Protocols and the Siemens protocols

	Siemens Protocol	Our Protocols
Protocol A	Flaws: Total messages are large.	Improve: Total messages are reduced.
Protocol B		Improve: Total messages are reduced.
Protocol C		Improve：The new protocol reduces the total messages.

Chapter 4 Conclusions and Future Research

In this thesis, we have proposed three new authentication mechanisms based on Asymmetric-key cryptosystems. In our study protocols, we have build up the authentication protocols that provide a good protection of ensuring the freshness of authentication data, session key and shared secret data. Another feature is the transmission data size within communications less than the protocols proposed by Siemens.

In the third generation mobile systems, there involves various services such as e-commence, Internet, computing data and so on. In this service, there are still lots of topics that are worthy to be explored in authentication protocols. They should be provided with different security considerations. In the future, we will continue to design new authentication protocols and will improve their performance by reducing the communication times during the process of authentication and also by reducing the transmission data size within communications.

Appendix A

A New Representation of Message Flow of Authentication Protocol

In the new representation of message flow of authentication protocol [28], the advantages of the new representation of message flow, are to assist us in recognizing the meaning of each message involved in the authentication protocol. In this new representation of message flow, it defines two notations: one is **challenge**, denoted by ▶or ◀; and **response** ▶▶or ◀◀. These two notations are used to describe the relationships between a challenge message and its corresponding response message. In other words, someone has received a challenge message in the current run of the protocol, and he must send back the corresponding response message if he wants to be authenticated by the one who sends the challenge message.

▶: One utters a challenge message based on its own beliefs.

▶▶: One utters a response message based on its own beliefs and new beliefs derived from the challenge message it has gotten.

The following is an example to assist us to understand by using these notations in representations of the message flow.

Two parties A and B share a secret key K_{AB}. If A wants to authenticate B, A generates a random number R_A as a nonce and send R_A concatenated with A's identity ID_A as a challenge message to B (see **Figure 1**).

Figure 1. Challenge message flow

When B has received the message $ID_A||R_A$, B can know that A sends a challenge message R_A to him. For achieving authentication from B to A, B must send back a response message based on his own belief that A shares K_{AB} with B. B generates a response message by using K_{AB} to encrypt the message $ID_A||R_A$ concatenated with B's identity ID_B as a response message to A (see **Figure 2**).

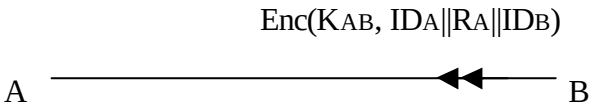

Figure 2. Response message flow

In the **Figure 2**, Enc(K, data) represents a symmetric key algorithm, by using key K to encrypt/decrypt data.

While A receives the message, A uses KAB to decrypt the received message $Enc(K_{AB}, ID_A||R_A||ID_B)$. A from the ciphertext is to retrieve ID_B. Then, A believes that B has shown his own belief to A in the current run of the protocol. A can make sure that the unilateral authentication of B to A has been achieved.

In the following, some types of transmission step, are shown and will used new representation of message flow.

Ordinary transmission step: To transmit data expect challenge and response data. The arrow represents the destination of transmitted data.

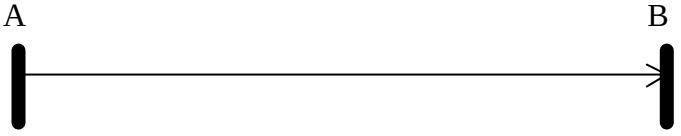

Figure 3. Ordinary transmission step

Challenge/Response transmission step: To transmit a pair of Challenge/Response data.

Figure 4. Challenge/Response transmission step

Parallel transmission step: To transmit a hybrid data including regular data, Challenge and Response data. The dotted line means that data 1 and data 2 are transmitted at the same transmission step.

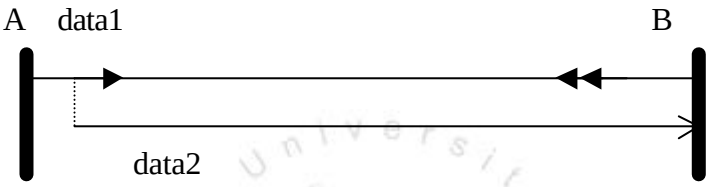

Figure 5. Parallel transmission step

Appendix B

A Security Threats And Requirement

In some instances, 3G will need to be equipped with stronger or more flexible security mechanisms than those which were designed for GSM, due to new or increased threats. These will be treated in the threat analysis.

Security threats

The purpose of this clause is to list possible security threats to the 3G systems, detailing what the threats achieve, how they are carried out and where in the system they could occur. It is possible to classify security threats in many different ways. In this clause threats in the following categories have been considered. We will introduce some security threats [30] relative to our thesis.

Unauthorized access to sensitive data (violation of confidentiality)

Eavesdropping: An intruder intercepts messages without detection.

Masquerading: An intruder hoaxes an authorized user into believing that they are the legitimate system to obtain confidential information from the user; or an intruder hoaxes a legitimate system into believing that they are an authorized user to obtain system service or confidential information.

Traffic analysis: An intruder observes the time, rate, length, source, and destination of messages to determine a user's location or to learn whether an important business transaction is taking place.

Browsing: An intruder searches data storage for sensitive information.

Leakage: An intruder obtains sensitive information by exploiting processes with legitimate access to the data.

Inference: An intruder observes a reaction from a system by sending a query or signal to the system. For example, an intruder may actively initiate communications sessions and then obtain access to information through observation of the time, rate, length, sources or destinations of associated messages on the radio interface.

Unauthorized manipulation of sensitive data (Violation of integrity)

Manipulation of messages: Messages may be deliberately modified, inserted, replayed, or deleted by an intruder.

Disturbing or misusing network services (leading to denial of service or reduced availability)

Intervention: An intruder may prevent an authorized user from using a service by jamming the user' s traffic, signalling, or control data.

Resource exhaustion: An intruder may prevent an authorized user from using a service by overloading the service.

Misuse of privileges: A user or a serving network may exploit their privileges to obtain unauthorized services or information.

Abuse of services: An intruder may abuse some special service or facility to gain an advantage or to cause disruption to the network.

Repudiation: A user or a network denies actions that have taken place.

Unauthorized access to services

Intruders can access services by masquerading as users or network

entities. Users or network entities can get unauthorized access to services by misusing their access rights.

A number of security threats in these categories are subsequently treated in the remainder of this clause according to the following points of attack:

-Radio interface.

- Other part of the system.

- Terminals and UICC/USIM.

Note also that Annex A gives some extra information as regards threats connected to active attacks on the radio interface. The threats treated in annex A are incorporated in the following lists.

Threats associated with attacks on the radio interface

The radio interface between the terminal equipment and the serving network represents a significant point of attack in 3G. The threats associated with attacks on the radio interface are split into the following categories, which are described in the following subclauses:

- Unauthorized access to data.

- Threats to integrity.

- Denial of service.

- Unauthorized access to services.

Unauthorized access to data

T1a **Eavesdropping user traffic:** Intruders may eavesdrop user traffic on the radio interface.

T1b **Eavesdropping signalling or control data:** Intruders may

eavesdrop signalling data or control data on the radio interface. This may be used to access security management data or other information, which may be useful in conducting active attacks on the system.

T1c **Masquerading as a communications participant:** Intruders may masquerade as a network element to intercept user traffic, signaling data or control data on the radio interface.

T1d **Passive traffic analysis:** Intruders may observe the time, rate, length, sources or destinations of messages on the radio interface to obtain access to information.

T1e **Active traffic analysis:** Intruders may actively initiate communications sessions and then obtain access to information through observation of the time, rate, length, sources or destinations of associated messages on the radio interface.

Threats to integrity

T2a **Manipulation of user traffic:** Intruders may modify, insert, replay or delete user traffic on the radio interface. This includes both accidental or deliberate manipulation.

T2b **Manipulation of signalling or control data:** Intruders may modify, insert, replay or delete signaling data or control data on the radio interface. This includes both accidental or deliberate manipulation.

NOTE: Replayed data, which cannot be decrypted by an intruder, may still be used to conduct attacks against the integrity of user traffic, signalling data or control data.

Denial of service attacks

T3a **Physical intervention:** Intruders may prevent user traffic, signaling data and control data from being transmitted on the radio interface by physical means. An example of physical intervention is jamming.

T3b **Protocol intervention:** Intruders may prevent user traffic, signaling data or control data from being transmitted on the radio interface by inducing specific protocol failures. These protocol failures may themselves be induced by physical means.

T3c **Denial of service by masquerading as a communications participant:** Intruders may deny service to a legitimate user by preventing user traffic, signalling data or control data from being transmitted on the radio interface by masquerading as a network element

Unauthorized access to services

T4a **Masquerading as another user:** An intruder may masquerade as another user towards the network. The intruder first masquerades as a base station towards the user, then hijacks his connection after authentication has been performed.

Threats associated with attacks on other parts of the system

Although attacks on the radio interface between the terminal equipment and the serving network represent a significant threat, attacks on other parts of the system may also be conducted. These include attacks on other wireless interfaces, attacks on wired interfaces, and attacks, which cannot be attributed to a single interface or point of attack. The threats associated with attacks on other parts of the system are split into

the following categories, which are described in the following subclauses:

- Unauthorized access to data.
- Threats to integrity.
- Denial of service.
- Repudiation.
- Unauthorized access to services.

Unauthorized access to data

T5a **Eavesdropping user traffic:** Intruders may eavesdrop user traffic on any system interface, whether wired or wireless.

T5b **Eavesdropping signalling or control data:** Intruders may eavesdrop signalling data or control data on any system interface, whether wired or wireless. This may be used to access security management data which may be useful in conducting other attacks on the system.

T5c **Masquerading as an intended recipient of data:** Intruders may masquerade as a network element in order to intercept user traffic, signalling data or control data on any system interface, whether wired or wireless.

T5d **Passive traffic analysis:** Intruders may observe the time, rate, length, sources or destinations of messages on any system interface, whether wired or wireless, to obtain access to information.

T5e **Unauthorized access to data stored by system entities:** Intruders may obtain access to data stored by system entities. Access to system entities may be obtained either locally or remotely, and may involve breaching physical or logical controls.

T5f **Compromise of location information:** Legitimate user of a 3G service may receive unintended information about other users locations through (analysis of) the normal signalling or voice prompts received at call set up.

Threats to integrity

T6a **Manipulation of user traffic:** Intruders may modify, insert, replay or delete user traffic on any system interface, whether wired or wireless. This includes both accidental and deliberate manipulation.

T6b **Manipulation of signalling or control data:** Intruders may modify, insert, replay or delete signalling or control data on any system interface, whether wired or wireless. This includes both accidental and deliberate manipulation.

T6c **Manipulation by masquerading as a communications participant:** Intruders may masquerade as a network element to modify, insert, replay or delete user traffic, signalling data or control data on any system interface, whether wired or wireless.

T6d **Manipulation of applications and/or data downloaded to the terminal or USIM:** Intruders may modify, insert, replay or delete applications and/or data, which is downloaded to the terminal or USIM. This includes both accidental and deliberate manipulation.

T6e **Manipulation of the terminal or USIM behaviour by masquerading as the originator of applications and/or data:** Intruders may masquerade as the originator of malicious applications and/or data downloaded to the terminal or USIM.

T6f **Manipulation of data stored by system entities:** Intruders may modify, insert or delete data stored by system entities. Access to

system entities may be obtained either locally or remotely, and may involve breaching physical or logical controls.

Denial of service attacks

T7a **Physical intervention:** Intruders may prevent user or signaling traffic from being transmitted on any system interface, whether wired or wireless, by physical means. An example of physical intervention on a wired interface is wire cutting. An example of physical intervention on a wireless interface is jamming. Physical intervention involving interrupting power supplies to transmission equipment may be conducted on both wired and wireless interfaces. Physical intervention may also be conducted by delaying transmissions on a wired or wireless interface.

T7b **Protocol intervention:** Intruders may prevent user or signalling traffic from being transmitted on any system interface, whether wired or wireless, by inducing protocol failures. These protocol failures may themselves be induced by physical means.

T7c **Denial of service by masquerading as a communications participant:** Intruders may deny service to a legitimate user by preventing user traffic, signalling data or control data from being transmitted by masquerading as a network element to intercept and block user traffic, signalling data or control data.

T7d **Abuse of emergency services:** Intruders may prevent access to services by other users and cause serious disruption to emergency services facilities by abusing the ability to make USIM-less calls to emergency services from 3G terminals. If such USIM-less calls are permitted then the provider may have no way of preventing the

intruder from accessing the service.

Repudiation

T8a **Repudiation of charge:** A user could deny having incurred charges, perhaps through denying attempts to access a service or denying that the service was actually provided.

T8b **Repudiation of user traffic origin:** A user could deny that he sent user traffic.

T8c **Repudiation of user traffic delivery:** A user could deny that he received user traffic.

Unauthorized access to services

T9a **Masquerading as a user:** Intruders may impersonate a user to utilize services authorized for that user. The intruder may have received assistance from other entities such as the serving network, the home environment or even the user himself.

T9b **Masquerading as a serving network:** Intruders may impersonate a serving network, or part of an serving network's infrastructure, perhaps with the intention of using an authorised user's access attempts to gain access to services himself.

T9c **Masquerading as a home environment:** Intruders may impersonate a home environment perhaps with the intention of obtaining information, which enables him to masquerade as a user.

T9d **Misuse of user privileges:** Users may abuse their privileges to gain unauthorized access to services or to simply intensively use their subscriptions without any intent to pay.

T9e **Misuse of serving network privileges:** Serving networks may abuse

their privileges to gain unauthorized access to services. The serving network could e.g. misuse authentication data for a user to allow an accomplice to masquerade as that user or just falsify charging records to gain extra revenues from the home environment.

Threats associated with attacks on the terminal and UICC/USIM

T10a **Use of a stolen terminal and UICC:** Intruders may use stolen terminals and UICCs to gain unauthorized access to services.

T10b **Use of a borrowed terminal and UICC:** Users who have been given authorization to use borrowed equipment may misuse their privileges perhaps by exceeding agreed usage limits.

T10c **Use of a stolen terminal:** Users may use a valid USIM with a stolen terminal to access services.

T10d **Manipulation of the identity of the terminal:** Users may modify the IMEI of a terminal and use a valid USIM with it to access services.

T10e **Integrity of data on a terminal:** Intruders may modify, insert or delete applications and/or data stored by the terminal. Access to the terminal may be obtained either locally or remotely, and may Involve breaching physical or logical controls.

T10f **Integrity of data on USIM:** Intruders may modify, insert or delete applications and/or data stored by the USIM. Access to the USIM may be obtained either locally or remotely.

T10g **Eavesdropping the UICC-terminal interface:** Intruders may eavesdrop the UICC-terminal interface.

T10h **Masquerading as an intended recipient of data on the**

UICC-terminal interface: Intruders may masquerade as a USIM or a terminal in order to intercept data on the UICC-terminal interface.

T10i **Manipulation of data on the UICC-terminal interface:** Intruders may modify, insert, replay or delete user traffic on the ICC-terminal interface.

T10j **Confidentiality of certain user data in the terminal or in the UICC/USIM:** Intruders may wish to access personal user data stored by the user in the terminal or UICC, e.g. telephone books.

T10k **Confidentiality of authentication data in the UICC/USIM:** Intruders may wish to access authentication data stored by the service provider, e.g. authentication key.

Requirements derived from threat analysis

This subclause gives a complete list of security requirements as derived from the threat analysis. They have not been ordered according to risk evaluation values. The threat or threats directly leading to the requirement or connected to the requirement are given in brackets for each entry.

Requirements on security of 3GPP services

Requirements on secure service access

R1a A valid USIM shall be required to access any 3G services except for emergency calls where the network should be allowed to decide whether or not emergency calls should be permitted without a USIM. (T7d, T9a,d)

R1b It shall be possible to prevent intruders from obtaining unauthorized access to 3G services by masquerading as authorized users. (T4a, T9a,c)

R1c It shall be possible for users to be able to verify that serving networks are authorized to offer 3G services on behalf of the user' s home environment at the start of, and during, service delivery. (T1c,e, T3c, T4a,T9b,c)

Requirements on secure service provision

R2a It shall be possible for service providers to authenticate users at the start of, and during, service delivery to prevent intruders from obtaining unauthorized access to 3G services by masquerade or misuse of priorities. (T4a, T8a, T9a,d)

R2b It shall be possible to detect and prevent the fraudulent use of services. Alarms will typically need to be raised to alert providers to security-related events. Audit logs of security related events will also need to be produced. (T8a,b,c, T9d,e, T10a,b)

R2c It shall be possible to prevent the use of a particular USIM to access 3G services. (T9a,d, T10a)

R2d It shall be possible for a home environment to cause an immediate termination of all services provided to certain users, also those offered by serving networks.(T9a,d, T10a,b)

R2e It shall be possible for the serving network to be able to authenticate the origin of user traffic, signaling data and control data on radio interfaces. (T8a,b,c, T9c)

Note: It is assumed that user traffic contains sufficient redundancy such that a stream cipher provides a basic level of data origin authentication on the radio interfaces and that, if that is not sufficient and additional measures are required, the application should be aware and measures

should be implemented at the application layer.

R2f It shall be possible to prevent intruders from restricting the availability of services by logical means.

(T3b,c, T7e)

R2g There shall be a secure infrastructure between **Network Operators**, designed such that the need for HE trust in the SN for security functionality is minimized.

Requirements on system integrity

R3a It shall be possible to protect against unauthorized modification of user traffic. (T2a, T6a,c, T7b,c)

Note: It is assumed that user traffic contains sufficient redundancy such that a stream cipher provides a basic level of data integrity protection on the radio interfaces and that, if that is not sufficient and additional measures are required, the application should be aware and measures should be implemented at the application layer.

R3b It shall be possible to protect against unauthorized modification of certain signalling data and control data, particularly on radio interfaces. (T2b, T3b,c, T6b,c, T7a,b,c)

R3c It shall be possible to protect against unauthorized modification of user-related data downloaded to or stored in the terminal or in the USIM. (T6d,e, T6c, T10f,i)

R3d It shall be possible to protect against unauthorized modification of user-related data, which is stored or processed by a provider. (T6c,f)

R3e It shall be possible to ensure that the origin and integrity of applications and/or data downloaded to the terminal and/or the

UICC can be checked. It may also be necessary to ensure the confidentiality of downloaded applications and/or data. (T6c,d,e,f, T10e,f,i)

R3f It shall be possible to ensure the origin, integrity and freshness of authentication data, particularly of the cipher key on the radio interface. (T1a,b, T2b, T5c, T6c)

R3g It shall be possible to secure infrastructure between operators. (T5a,b,c, T6a,b,c, T7a,b,c, T9b,c)

Requirements on protection of personal data

Security of user-related transmitted data

R4a It shall be possible to protect the confidentiality of certain signaling data and control data, particularly on radio interfaces. (T1b,d, T5b,c,d)

R4b It shall be possible to protect the confidentiality of user traffic, particularly on radio interfaces. (T1a, T5a)

R4c It shall be possible to protect the confidentiality of user identity data, particularly on radio interfaces. (T1b,d, T3b, T5b,c,d,e)

R4d It shall be possible to protect the confidentiality of location data about users, particularly on radio interfaces. (T1b, T3b, T5b,c,d,e)

R4e It shall be possible to protect against the unwanted disclosure of location data for a user participating in a particular 3G service to other parties participating in the same 3G service. (T5f)

R4f It shall be possible for the user to check whether or not his user traffic and his call related information is confidentiality protected. This should require minimal user activity. (T1a,b)

Security of user-related stored data

R5a It shall be possible to protect the confidentiality of user-related data which is stored or processed by a provider. (T5c,e)

R5b It shall be possible to protect the confidentiality of user-related data stored by the user in the terminal or in the USIM. (T10h,j)

Requirements on the terminal/USIM

USIM Security

R6a It shall be possible to control access to a USIM so that it can only be used to access 3G services by the subscriber to whom it was issued or by users explicitly authorized by that subscriber. (T10a, g)

R6b It shall be possible to control access to data in a USIM. For instance, some data may only be accessible by an authorized home environment. (T10h,j, k) R6c. It

shall not be possible to access data in a USIM that is only intended to be used within the USIM, e.g. authentication keys and algorithms. (T10h,k)

Terminal Security

R7a It shall be possible to deter the theft of terminals. (T10a,c,d)

R7b It shall be possible to bar a particular terminal from accessing 3G services. (T10a,c,d)

R7c It shall be difficult to change the identity of a terminal to circumvent measures taken to bar a particular terminal from accessing 3G services. (T10a,c,d)

Appendix C

General objectives for 3G security features

The general objectives for 3G security features have following entries:

(a) To ensure that information generated by or relating to a user is adequately protected against misuse or misappropriation.

(b) To ensure that the resources and services provided by serving networks and home environments are adequately protected against misuse or misappropriation.

(c) To ensure that the security features standardized are compatible with world-wide availability (There shall be at least one ciphering algorithm that can be exported on a world-wide basis (in accordance with the Wassenaar agreement)).

(d) To ensure that the security features are adequately standardized to ensure world-wide interoperability and roaming between different serving networks.

(e) To ensure that the level of protection afforded to users and providers of services is better than that provided in contemporary fixed and mobile networks.

(f) To ensure that the implementation of 3G security features and mechanisms can be extended and enhanced as required by new threats and services.

Furthermore it has been agreed that the basic security features employed in 2G systems will be retained, or where needed enhanced. These include:

- Subscriber authentication.

- Radio interface encryption.
- Subscriber identity confidentiality.
- Use of removable subscriber module.
- Secure application layer channel between subscriber module and home network.
- Transparency of security features.
- Minimized need for trust between HE and SN.

Reference

[1] A. T. Khalid and A. Ali, "A new authentication protocol for Roaming users in GSM Network," *IEEE International Symposium on Computers and Communications Proceedings*, pp.93-98, 1999.

[2] V. Bharghavan and C. V. Ramamoorthy, "Security Issues in Mobile Communications," Second International Symposium on Autonomous Decentralized Systems Proceedings. ISADS 95, pp.19-24, 1995.

[3] J. Liu and Y. Wang, "A User Authentication Protocol for Digital Mobile Communication Network," *Wireless: Personal, Indoor and Mobile Radio Communications Merging onto the Information Superhighway, PIMRC'95. Sixth IEEE International Symposium* , Vol.2 , pp.608-612, 1995.

[4] W. Stallings, Cryptography and network security principles and practice, 2nd ed, Prentice Hall, Inc, 1999.

[5] ETSI TS 133.120. "3G Security", http://www.etsi.org/

[6] ETSI TS 21.133."Security Threats and Requirements, http://www.etsi.org/

[7] C. S. Park, "On certificate-based security protocols for wireless mobile communication systems," *IEEE Network*, Vol.115, pp.28-32, Oct 1997.

[8] N Jefferies, "Security in third-generation mobile systems," *IEEE Colloquium on Security in Network*, pp.8/1-8/5, 1995.

[9] C. Metz, "AAA protocols: authentication, authorization, and accounting for the Internet," *IEEE Internet Computing*, Vol.36, pp. 75-79,

Nov.-Dec. 1999.

[10] S. Putz, R. Schmitz and F. Tonsing, "Authentication schemes for third generation mobile radio systems," *The Ninth IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, Vol. 1, pp.126-130, 1998.

[11] S. M. Yen, "Cryptanalysis of an authentication and key distribution protocol," *IEEE Communications Letters*, Vol.31, pp.7-8, Jan 1999.

[12] Z. Zheng, N. Zhang, "Dynamic Authentication Protocol for Personal Communication System (PCS)," *International Conference on Communication Technology, ICCT'98*, Beijing, China, pp.7-1-7-5, Oct 1998.

[13] V. Varadharajan and M. Yi, "Preserving privacy in mobile communications: a hybrid method," *IEEE International Conference on Personal Wireless Communications*, pp.532-536, 1997.

[14] B.Askwith, M. Merabti, Qi Shi, K. Whiteley, "Achieving user privacy in mobile networks," *Proceedings of the 13th Annual Computer Security Applications Conference*, pp.108-116, 1997.

[15] R. Bird, I. Gopal, A. Herzberg, P. A. Janson, S. Kutten, R. Molva, M. Yung, "Systematic design of a family of attack-resistant authentication protocols," *IEEE Journal on Selected Areas in Communications*, Vol.115, pp.679-693, June 1993.

[16] T. G. Brutch and P. C. Brutch, "Mutual Authentication, Confidentiality, and Key MANagement (MACKMAN) system for mobile computing and wireless communication," *Proceedings of the 14th Annual Computer Security Applications Conference*, pp. 308-317, 1998.

[17] L. Gong, M.A. Lomas, R.M. Needham, J.H. Saltzer, "Protecting

poorly chosen secrets from guessing attacks," *IEEE Journal on Selected Areas in Communications*, Vol.115, pp.648-656, June 1993.

[18] S. Keung and K. Y. Siu, "Efficient protocols secure against guessing and replay attacks," *Proceedings of the Fourth International Conference on Computer Communications and Networks*, pp.105-112, 1995.

[19] T. Kwon and J. Song, "Authenticated key exchange protocols resistant to password guessing attacks," *IEEE Proceedings of Communications* , Vol.1455, pp.304-308, Oct 1998.

[20] G. Li, "Optimal authentication protocols resistant to password guessing attacks," *Proceedings of the Eighth IEEE Computer Security Foundations Workshop*, pp.24-29, 1995.

[21] S. P. Shieh, W. H. Yang and H. M. Sun, "An authentication protocol without trusted third party," *IEEE Communications Letters*, Vol.13, pp.87-89, May 1997.

[22] K. Heikki, A. Ari, N. Valtteri, L. Lauri, N. Siamak, UMTS Network: Architecture, Mobility and Services, Wiley, Inc, 2001.

[23] J. Rapeli, "UMTS: targets, system concept, and standardization in a global framework," *IEEE Personal Communications*, Vol.2(1), pp.20-28, Feb 1995.

[24] Y. B. Lin, "Mobility management for PCS," *Tutorial: First Workshop on Mobile Computing, Applied Research, Bellcore Morristown*, NJ, USA, 1995.

[25] **賴溪松, 韓亮, 張真誠, 近代密碼學及其應用, 松岡電腦圖書**, 1994.

[26]Y. B. Lin, " No wires attached," *IEEE Potentials* ," Vol. 14 Issue: 4 ,

pp.28 –33, Oct.-Nov. 1995.

[27] F. G. Constantinos, I. M. Sotirios and S. V. Iakovos, “Towards the Introduction of the Asymmetric Cryptography in GSM, GPRS, and UMTS Networks,” *Computers and Communications, 2001. Proceedings. Sixth IEEE Symposium*, pp.15-21, 2001.

[28] **張鴻泰**, “UMTS **認證協定之研究**,” M.S.Thesis, Dept. of electrical engineering, Chung Yuan Christian University, 2000.

[29] http://www.esat.kuleuven.ac.be/cosic/aspect/aspect.html

[30] ETSI TS 121.133.”Security Threats and Requirements, http://www.etsi.org/

[31] W. Diffie, M. Hellman, “New directions in cryptography,” *IEEE Transactions on Information Theory*, pp.644-654, 1976.

[32] R. Moe, “Overview of the GSM system and protocol architecture,” *IEEE Communication Magazine*, pp. 92-100, April 1993.

[33] B. Schneier, “Applied cryptography: Protocols , algorithms, and source code in C,” Wiley.

[34] R. Bird et al., “Systematic Design of Two-Party Authentication Protocols,” Advances in Cryptology-CRYPTO’ 91, pp. 44-61, 1991.

[35] G. Li, “Optimal authentication protocols resistant to password guessing attacks,” *Proceedings of Eighth IEEE on Computer Security Foundations Workshop*, pp.24-29, 1995.

[36] G. Tsudik, E. Herreweghen, “Some remarks on protecting weak keys and poorly-chosen secrets from guessing attacks,” *Proceedings of The 12th Symposium on Reliable Distributed Systems*, pp.136-141, 1993.

[37] G. Lowe, “Some new attacks upon security protocols,” Proceedings

of The 9th *IEEE on Computer Security Foundations Workshop*, pp.162-169,1996.

[38] L. Gong, "Verifiable-text attacks in cryptographic protocols." *Ninth Annual Joint Conference of the IEEE Computer and Communication Societies*, Vol.2, pp.686-693,1990.

[39] P. Syverson, "A taxonomy of replay attacks," *Proceedings of Computer Security Foundations Workshop VII*, pp.187-191, 1994.

[40] S. Keung, K. Y. Siu, "Efficient protocols secure against guessing and replay attacks," *Proceedings of Fourth International Conference on Computer Communications and Networks*, pp.105-112, 1995.

[41] T. Kwon, J. Song, " Security and efficiency in authentication protocols resistant to password guessing attacks," *Proceedings of The 22nd Annual Conference on Local Computer Networks*, pp.245-252, 1997.

[42] Y. Zheng, J. Seberry, "Immunizing public key cryptosystems against chosen ciphertext attacks," *IEEE Journal on Selected Areas in Communications*, Vol.11, NO.5, pp.715-724, June 1993.

作者簡介

姓名：林志興

出生：民國 66 年 2 月 5 日

籍貫：台灣省宜蘭縣

學歷：86 年畢業於復興工專電機工程科

89 年畢業於明新技術學院電機工程學系

91 年畢業於中原大學電機工程學系研究所

住址：宜蘭市渭水路三十四之四號

電話：(03) 9323935