國 立 交 通 大 學

資 訊 工 程 學 系

碩 士 論 文

3G 網路的匿名行動付款

Anonymous Mobile Payment for 3G Networks

指導教授：張明峰 博士

研 究 生：黃逸聖

中華民國九十三年六月

3G 網路的匿名行動付款

Anonymous Mobile Payment for 3G Networks

研 究 生：黃逸聖　　Student: Yi-Sheng Huang
指導教授：張明峰博士　　Advisors: Dr. Ming-Feng Chang

國 立 交 通 大 學
資 訊 工 程 學 系
碩 士 論 文

A Thesis Submitted to
Department of Computer Science and Information Engineering
College of Electrical Engineering and Computer Science
National Chiao Tung University
in Partial Fulfillment of the Requirements
for the Degree of Master
in
Computer Science and Information Engineering
June 2004
Hsinchu, Taiwan, Republic of China

中華民國九十三年六月

3G 網路的匿名行動付款

學生：黃逸聖　　指導教授：張明峰 博士

國立交通大學資訊工程學系（研究所）碩士班

摘要

行動付款是指使用者利用行動設備如手機及行動服務提供者所提供的付款方式來進行行動商務。由於目前已經是人手一機及 3G 網路的即將到來的狀況下，行動付款服務已經漸漸的吸引眾多的付款服務提供者的注意。目前由行動網路服務業者提供行動付方式可分即時扣款的預付卡(Prepaid)及每月結帳(Postpaid)兩項方式，並且第三方如銀行可視為付款服務提供者的延伸，因此第三代行動網路服務業者適合扮演付款服務提供者的角色，並且可以結合 3G 所提供的身份確認的機制以提供完整的行動付款服務。

在本論文中，我們將匿名行動付款的功能整合至 3G 網路中，設計 AAA 伺服器處理使用者的行動服務註冊及付費的資訊及提供用戶臨時代號 (Provisional Identity) 以支援匿名付款機制，加值服務業者可經由行動網路業者對客戶執行身份認證。並且使用記帳及付款閘道器 (Charging/Payment Gateway)與 3G 網路所提的即時付帳系統 (Online Charging System)、每月結帳系統 (Offline Billing System) 以及第三方的帳務系統介接，讓使用者在行動商務時可以利用預付卡，每月結帳或者透過第三方如銀行轉帳的行動付費方式付款給加值服務業者。

Anonymous Mobile Payment for 3G Networks

Student: Yi-Sheng Huang Advisor: Dr. Ming-Feng Chang

Department of Computer Science and Information Engineering

National Chiao Tung University

ABSTRACT

Mobile payment means a user can make a payment with a mobile device through the payment methods provided by a mobile payment service provider. Almost everyone has at least one mobile phone and mobile network operators are deploying 3G networks; many mobile payment service providers are eager to provide service. The mobile payment services, prepaid and postpaid, provided by a network operator and mobile payment service can be extended to integrate with a third party, such as banks. Therefore, a network operator can be the mobile service provider.

In this thesis, an anonymous mobile payment scheme is integrated into 3G mobile networks. We design an AAA (Authentication, Authorization, and Accounting) server to handle user registration and payment procedure; a merchant can authenticate a customer through the network operator. The AAA server also provides each user a provisional identity to support anonymous payment. A CPGW (Charging/Payment Gateway) connects to the Online Charging System, Offline Billing System and the third party financial institutes. When a user makes a payment in the mobile commerce, the user can select prepaid, postpaid or third party account, such as a bank account to pay the payment for the merchants.

誌謝

首先要感謝張明峰老師的費心指導下，得以完成此論文的著作及實作。在這兩年期間老師的督促及訓練獨立思考研究，讓我無論在作研究或者做人處事方面成長了很多，謝謝老師辛勞的教誨。

還有要感謝網路通訊實驗室所成員的指教及關心，讓我可以在研究所這段期間的生活增添不少色彩。另外，在資工系計中和助教們彼此間的互相學習，讓我也更是懷念這樣難能可貴的學習環境及人事物。在這感謝你們，也很高興能夠認識你們！

最後謹在此將論文獻給我最親愛的家人們及珊珊，由於你們的支持，讓我可以工作之後重回學校求學的過程中一路順坦，沒有後顧之憂的完成學業。

Tables of Contents

List of Tables

List of Figures

Chapter 1 Introduction

1.1 Overview

Mobile communications have grown rapidly in the past ten years. For example, the penetration rate of mobile phones is over 100% in Taiwan, i.e., many people have more than one mobile phone. The total number of mobile phones has outnumbered that of personal computers worldwide. In addition to mobile telephone service, mobile network operators have also been promoting mobile data service, such SMS (Short Message Service) and GPRS (General Packet Radio Service). Mobile network operators expect mobile data service can be the next big wave. For now, mobile data service is still at the initial stage with limited success. The DoCoMo i-mode service and the number of short messages transmitted worldwide have increased exponentially. The highly promoted mobile service based on WAP (Wireless Access Protocol) does not realize because of the long transmission delay.

Mobile phones have become personal goods that every person owns. In addition to providing telephone communications at any place, anytime, mobile users in Europe can use mobile phones to buy soft drink from a vending machine, and pay parking fee or gasoline charge. Mobile network operators have a large base of subscribers and a well functioning charging and billing system; they hold the upper hand on making mobile phones as the payment tool for mobile commerce. Mobile network operators can be the banks in mobile commerce. From the user's viewpoints, using mobile phones as a mobile payment tool offers the following advantages: ubiquity, security, localization, convenience, and personalization. However, mobile phones also have limitations, such as limited memory capacity and computation power.

Mobile payment is an extension of electronic payment; at present, there are more than

one hundred of electronic payment schemes. Electronic payments can be classified into credit type and debit type payments. The debit type includes electronic cash, electronic check, and bank transfer, etc. Since cash must be deposited in advance, the debit type payments are similar to prepaid accounts in mobile networks. On the other hand, the credit type electronic payments are similar to postpaid accounts; both receive and pay monthly bills.

In the future, more mobile devices, such as mobile phones, Personal Digital Assistant (PDA) etc., will be used to make a the payment. If we use devices equipped with SIM/USIM cards, we can have a general mobile payment scenario to do the mobile commerce under the Third Generation (3G) UMTS (Universal Mobile Telephone Service) security architecture [10]. UMTS is a 3G Mobile System developed by ETSI

This thesis is organized as follows. The remaining of this chapter describes the motivation behind anonymous mobile payment solutions. Chapter 2 presents authentication method, charging principles of 3G UMTS and mobile payment concept. Chapter 3 looks at the anonymous mobile payment in the architecture of our solution. The fourth chapter presents how the system is implemented. The final chapter gives conclusions and describes future work.

1.2 Motivation

Important issues that must be considered in electronic payment include the amount of the payment, anonymity, security, and on-line or off-line validation. Electronic payments should protect the customer’s privacy, just as the merchants do not know the identity of a customer in a cash transaction. The security issues of electronic payment include integrity, authentication, authorization, confidentiality, availability, and reliability. The security issues described above require cryptographic technologies. For electronic payments using off-line verification, no

third party is involved besides the merchant and the customer. On the other hand, for those using on-line verification, a trusted third party, such as a bank or a network operator, is involved. On-line verification needs more messages exchanged, but can prevent the users from double spending.

Current mobile phone users can buy goods by dialing a premium-rate number; network operators charged the users based on the number dialed. For example, using the Mobile Pay provided by Sonera [1], a mobile user dials the number displayed on a vending machine to buy goods from it. Moreover, mobile handsets are used to authenticate the users and to obtain authorization from the user for a payment. Movilpago, Spain, provides merchants terminals, through which a customer's mobile phone number and the code of the purchased goods are input. The customer's handset will show the price and the description of the goods. After the customer enters his or her PIN to the handset, the network operator sends transaction confirmation messages to both the merchant and the customer. Paybox and GiSMo [1] use similar scheme to support mobile commerce.

The mobile commerce examples described above are based on the telephone number of a user to ensure a limited level of user authentication. MobilePay and MobileSmart use the caller identity information provided in the IN. Movilpago, Payboxand GiSMo the callee identity. Each transaction requires at least one phone call connected, or one short message transferred. The mobile network of next generation will be an all-IP network. User authentication based on the caller or callee ID is inadequate for the dynamic mobile commerce. Neither the anonymity requirement for mobile commerce is satisfied by current solutions, since the phone number of the customer is revealed to the merchants. Another limitation of the mobile commerce schemes above is that a mobile user can only purchase goods or value-added service from merchants who have signed contracts with the network operator. Due to the rapid development of wireless LANs, in the near future, there may be numerous independent small wireless networks based on 802.11 wireless LAN. In the

independent small networks, value-added services, such as printers, can be provided. To enable a mobile user to buy any products or obtain any service, in any networks, from any merchants (contracted or non-contracted) is an important issue.

The goal of this thesis is to design a charging and payment gateway and an AAA server for mobile networks to enable mobile users to purchase value-added service and goods using their mobile phones. The existing user authentication mechanism of mobile networks is reused for this mobile payment, and the VASP (value-added service provider) or merchant is paid by the network operators, which in turn charge the users for the transactions. Both postpaid users and prepaid users are supported. Moreover, the third parties can be involved through the charging and payment gateway.

1.3 Related work

Payment for mobile network usage can be classified into two categories: postpaid and prepaid. For a postpaid user, the CDRs (call detail records) generated by the mobile switches for each phone call are used to produce the monthly bills. A CDR [5] contains the information of a phone call, including the calling party, the called party, the date and time, the duration, the types of the call, etc. The CDR of a mobile phone call includes additional information, such as location area, cell ID, radio channel and the IMEI (International Mobile Equipment Identity). An MSC sends the CDRs in batch, usually during the off-peak hours, to a central CDR database. The billing system retrieves the CDR database, rates each call and generates the monthly bills for the subscribers.

The charging and billing of mobile data network, such as GPRS network, and its value-added services are based one the extensions of current CDR system. Take GPRS for example, the nodes of GPRS core network, SGSN and GGSN, generate mobility management

CDR (M-CDR records user location), SGSN CDR (S-CDR records radio channel usage and QoS) and GGSN CDR (G-CDR records the data volume with external IP network) [5]. The CDRs are relayed by the CGF (Charging Gateway Function) [5] to the billing system. In addition, 3G UMTS define even more types of CDRs to support the charging and billing system.

There are four approaches to provide mobile prepaid service: hot billing, service node, IN (Intelligent Network) and handset-based. The hot billing and the handset-based approaches provide solutions without major changes to the network infrastructure. Intelligent network solution offers real time rating and real time call control, but is not widely deployed today. The service node approach, which utilizes extra voice circuits and switching resources for prepaid calls, provides a variant to the intelligent network solution. The mobile data networks, GPRS and UMTS, extend the IN approach to support prepaid services. The ETSI have defined CAMEL (Customized Application for Mobile Enhanced Logic) phase 3 for service control of short messages and packet data.

1.4 Summary

In this thesis, it provides a few basics about mobile payment and charging principles for the 3G Networks. And finally, some payment solutions will be offered that can strengthen the 3G charging principles. In this mechanism, the architecture does not use special hardware or modify the architecture of 3G UMTS networks that the specification has defined. These allow users to issue the payment for their purchase or content downloading and keep their privacy. By using the 3G UMTS security, it provides the network access security to users with secure access to 3G services.

Chapter 2 3G Networks Security Architecture and Charging Principles

In this chapter, we will introduce 3G network security and charging principles. Security assures the reliability that consumers who use a mobile device purchase the good. Charging principles define how to charge the users when they use the network resources. 3G network provides payment methods, such as prepaid and postpaid, to charge the users when they use the network resources. The users can pay the network operators by a prepaid account or postpaid account. Moreover, the users can pay through an account of a third party, such as a bank, if the network operators cooperate with the third parties. We will also discuss mobile payment. We will introduce how mobile payment can be performed by using these payment methods provided by the mobile payment service provider and how payment service providers can be integrated with 3G network operators.

2.1 3G Security Architecture Overview

2.1.1 Security

Security protects our payment transactions from stealing and keeps them integrity [3]. Integrity means that there is no any duplication and modification in the message from a sender to a receiver. It is the most important issue not only for the network operators but also for users, especially in the financial accounting. The network operators and users all hope they do not have to bear the compensability to pay the money if someone fakes. There are many payment methods for purchasing goods, such as credit cards, cash and checks. We can use

these payment methods to buy something we need directly, through the Internet, mail-order, or fax. They also provide some security feature; some require signature to authenticate the user, and it is hard to forge the coin and paper money. We can see the success of using SIM card to authenticate users in GSM. SIM card is one kind of smart card. There is a small chip in the SIM card. It is difficult to crack a SIM card to get the information of the user. So we can use the mobile phone to communicate with someone securely.

The solution to the secure service should include principles as follow,

- Confidentiality: Protect the data from attacks
- Authentication: Assure that the user is valid and can use resource
- Integrity: Assure that the data is complete and prevent from being duplicated and modified.
- Nonrepudiation: The sender or receiver cannot deny the transaction they made.
- Access control: give every user his or her own privilege
- Availability: The protection used to enhance the system more secure, such as authentication and encryption. When the system loses some protection, it can be recovered from the backup data.

2.1.2 3G Network Security

Four level security features [9] for 3 G networks have been defined as shown in Figure 2-1.

a、Network access security (see Figure 2-1 (I)):

To provide users with secure access to 3G services and protect against attacks on the radio access link.

b、Network domain security (see Figure 2-1 (II)):

To provide entities in the network domain to securely exchange data packets and protect against attacks on the wireline network. We can use IPSec or TSL to enhance network domain

security.

c、User domain security (see Figure 2-1 (III)):

When a user wants to access or operate the mobile stations, the user and USIM can share a secret Personal Information Number (PIN).

d、Application security (see Figure 2-1 (IV)):

Provide applications security of exchanging messages between the user and the provider domain. USIM Application Toolkit (USAT) can be used to develop security mechanism.

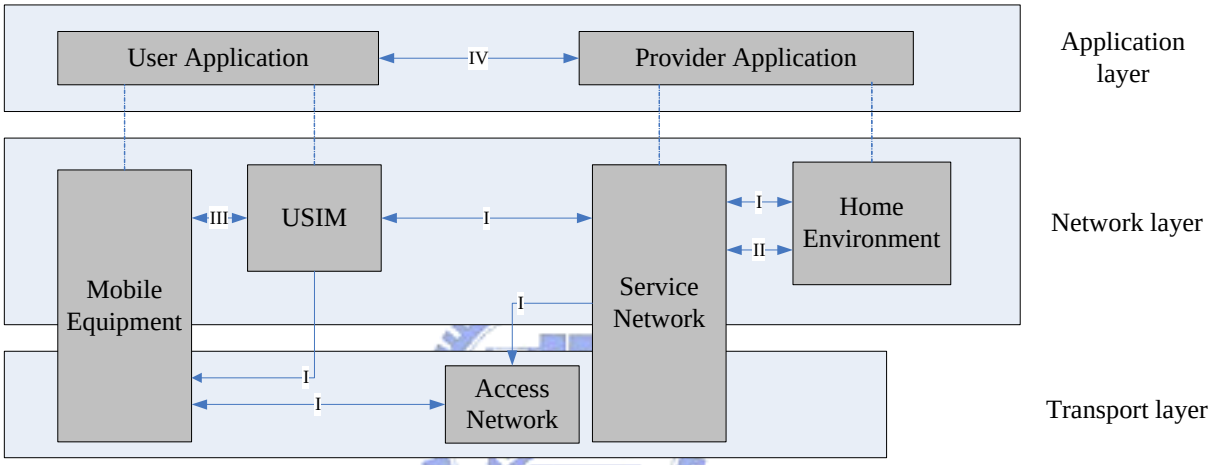

Figure 2-1: Overview of the security architecture

In the Internet, we can use credit card or prepaid cards to make a payment through a PC, what is so called the e-commerce or e-payment. E-payment just provides payment methods, but it still needs security features to protect the session that transfers financial data in the Internet. The secure methods used to protect the session are TLS and SET, TLS and SET are based on Public Key algorithms which need more computing power than private key algorithms.

Contrary to the e-payment, mobile payment means that the users use mobile devices equipped with a SIM card in the 3G networks to make a payment. A network operator as the mobile service provider not only provides basic radio access network security but also provides complete billing system of various charging or payment for the users. The network operators provide Postpaid (Offline Charging) and Prepaid (Online Charging) [5, 6, 7, 8].

Moreover, they can cooperate with a third-party like a bank. They can provide many payment methods and users can choose what they need or what they like to pay, it is more convenient to pay with their mobile device than e-payment.

2.1.3 User Authentication of 3G Networks

The specialty in the mobile network is to use a SIM/USIM card. The user's private key K is stored in a SIM/USIM card. The user authenticates towards the network with authentication and key agreement based on the secret key K shown in Figure 2-2. A lot of processes of cipher algorithm agreement should be passed between a mobile station and the network.

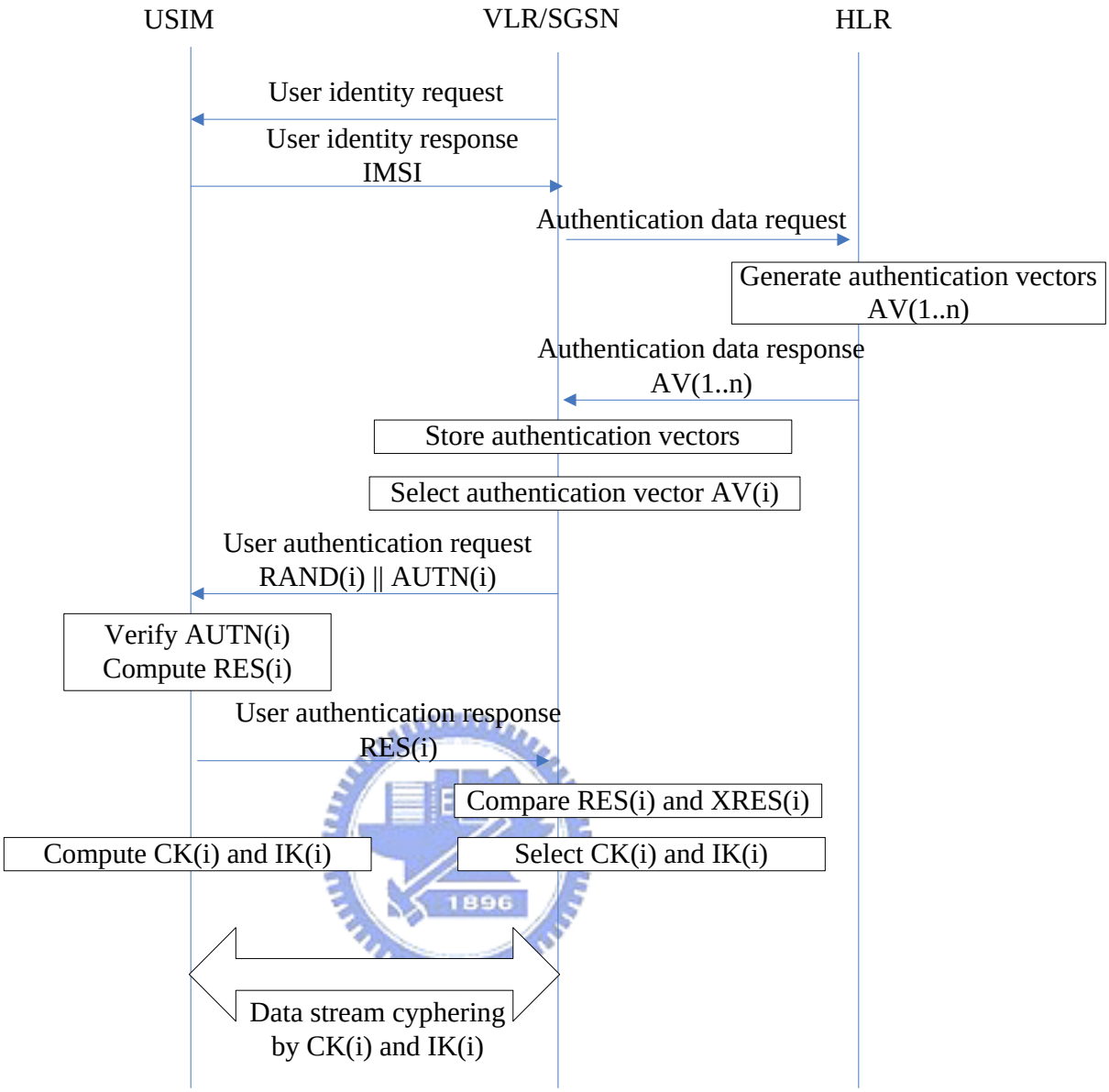

Figure 2-2: Authentication and key agreement

3G provides the following security features for the radio link:

- IMSI confidentiality when users access the network
- IMSI authentication when users register to the network
- User data confidentiality on physical connections by ciphering
- Connectionless user data confidentiality by ciphering

The security mechanism in 3G uses cipher keys. It means that stream cipher uses a derived cipher key, CK and IK. Sequence numbers in authentication vectors protect against reuse of authentication vectors.

2.2 3G Mobile Network Charging Architecture

The 3rd Generation charging architecture is logically divided into two domains, the Circuit Switch (CS) domain and the Packet Switch (PS) domain as shown in Figure 2-3. Moreover, it provides IP Multimedia Subsystem (IMS). 3G means The Third Generation mobile communication systems which provide higher data transfer rate than 2G. Circuit switched calls can be charged in one MSC server (the anchor MSC server) where all relevant data CDR is available and some CDR produced from HLR can also be used. The usage of the Packet Switch domain network can be charged in the information collected for each mobile station by SGSN and GGSN which serve that mobile station.

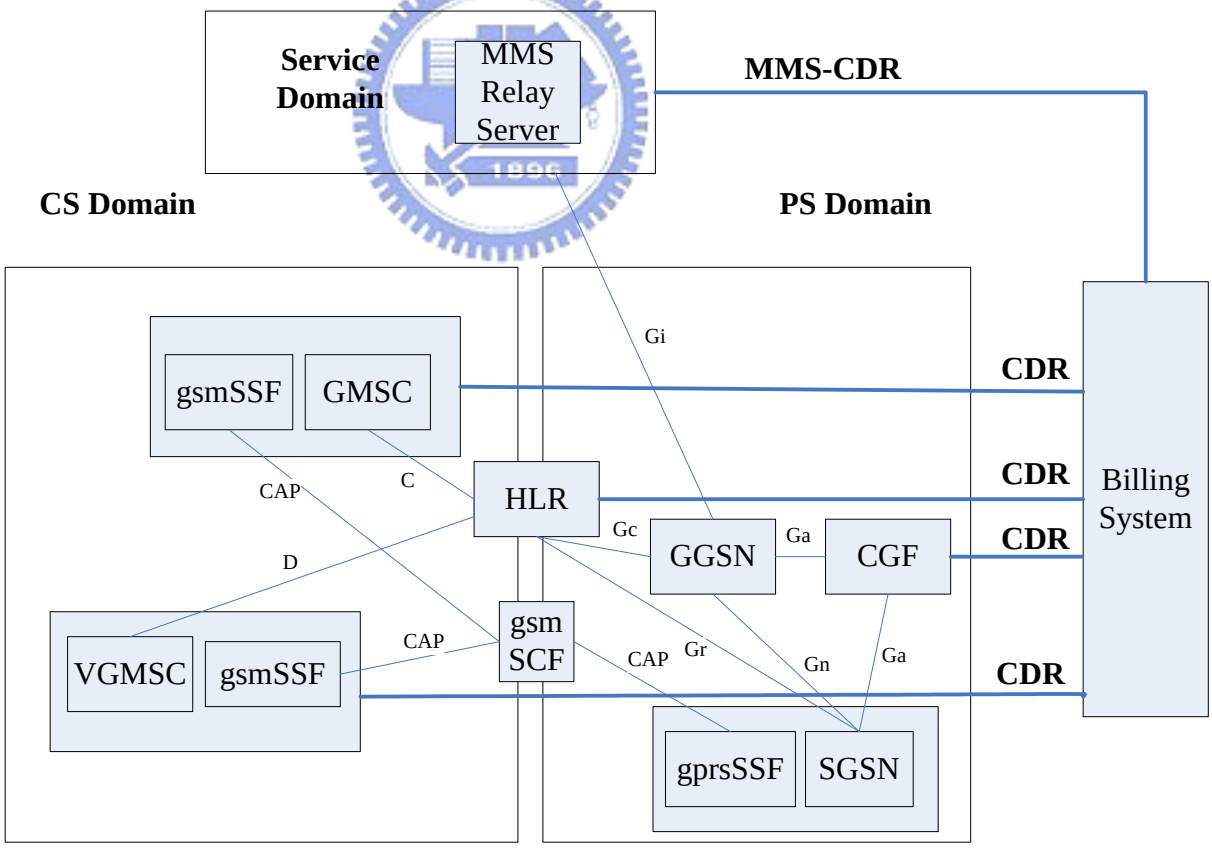

Figure 2-3: Overview of the 3G charging architecture

Charging is an accounting process of apportion between the Home Environment, Serving

Network and User. In 3G specifications, they define all charging scenarios how to charge users if they use the resource of the communication such as setting up a phone call or using the SMS, MMS. Some users like some business persons favor to pay the bill every month; and some users like children favor prepay their expense by their parents. We can call Postpaid or Offline Charging for paying the bill every month and Prepaid or Online Charging for pay the bill near to the real time.

2.2.1 Circuit Switch Domain

Circuit switch domain provides the voice service we use very often now. The MSC servers are responsible for the collection of all charging information for each mobile station or PSTN connection.

CDRs should be produced in several call scenarios.

- Mobile originated call attempt;
- Mobile originated emergency call attempt;
- Mobile originated, call forwarding attempt;
- Mobile terminated call attempt;
- Roaming call attempt in a gateway MSC server;
- Incoming call attempt in a gateway MSC server;
- Outgoing call attempt from a gateway MSC server;
- Transit call attempt;
- Terminating CAMEL call attempt;
- Supplementary service actions;
- HLR interrogation;
- Location updating;

- Short message service, mobile originated;
- Short message service, mobile terminated;
- Short message service, mobile originated interworking MSC server;
- Short Message service, mobile terminated gateway MSC server;
- Common equipment usage.

2.2.2 Offline and Online Charging in the Circuit Switch Domain

In offline charging, Charging Data Record (CDR) is the most important role. Offline charging is like postpaid in GSM. The more CDR it is produced, the more preferential payment, detailed bill or other value added services the network operator can provide to users.

Online charging service lived up to its name can charge user online. In GSM, it calls prepaid service. Now, prepaid service takes IN solution. In 3G, it specifies to use CAMEL. A CAMEL service can be activated for originating, forwarded, terminated calls and originating Short Message Service (SMS). In other words, CAMEL can be used to supplementary services, call forwarding, call hold, multi-party services and etc. Online Charging is one of theses services CAMLE can provide.

2.2.3 Packet Switch Domain

Packet Switch domain means that it can provide data packet services to users and it is similar to use internet by the personal computer. Core network add two new entities, SGSN and GGSN, in GPRS network.

2.2.4 Offline and Online Charging in the Packet Switch Domain

GSNs can collect some information about the usage of the radio interface, the usage duration, the usage of general Packet-Switched domain resources, destination and source, the usage of the external data networks and location of Mobile Station.

GSNs should generate these records of charging information

- Charging Data in the SGSN (S-CDR)
- Charging Data in the GGSN (G-CDR)
- Mobile Station Mobility Management Data in SGSN (M-CDR)
- SMS Mobile Originated Data in SGSN (S-SMO-CDR)
- SMS Mobile Terminated Data in SGSN (S-SMT-CDR)

CAMEL also supports Packet-Switch domain. The subscription information for the SGSN PDP context and mobile originated SMS is stored in HLR. Control point for the Online Charging services is in the gprsSSF entity and co-work with SGSN.

2.2.5 IP Multimedia Subsystem (IMS)

The IP Multimedia Subsystem consists of the core network elements provide multimedia services such as voice, video, message and web-base technologies. IP Multimedia sessions use IP connectivity bears to transport multimedia signaling and data traffic, and services are based on an IETF defined session control capability which utilized the PS domain as multimedia bearers. It may include some equivalent set of services to the CS domain. The IMS utilized the PS domain to transport multimedia signaling and bearer. The PS domain maintains the services while the mobile device moves and hides these moves from the IMS. IMS is independent to the CS domain. It means that it is not necessary to deploy CS domain

in order to support an IMS network.

IMS also specifies charging principles for all communications between the IMS network entities and Charging Function. In the Offline Charging, it uses Rf interface between CCF and the other entities; in the Online Charging, it uses Ro interface between ECF and other entities.

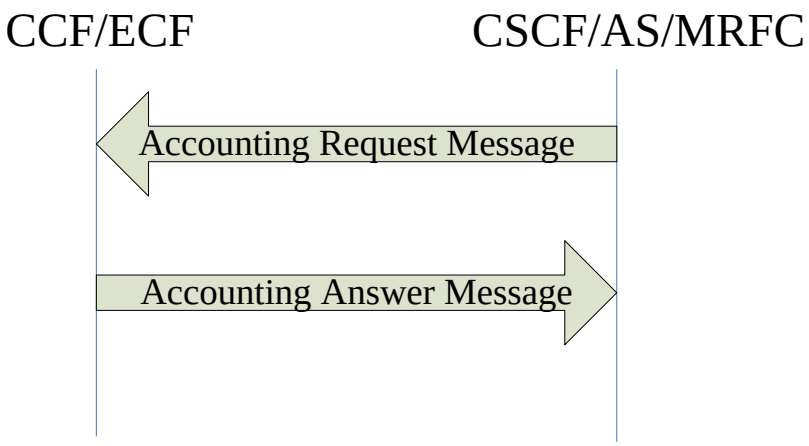

Figure 2-4: The charging interface of IMS

2.2.6 Offline and Online Charging in the IMS

Offline Charging is also based on the CDR. When a service starts or stop, the entities will send a request to Charging Collection Function (CCF). CCF will create relative CDR. CCF collections CDR and send this information to the Billing System (BS). Charging Gateway Function (CGF) also collects the CDR from GGNS and SGSN, it charges for the bearer resource.

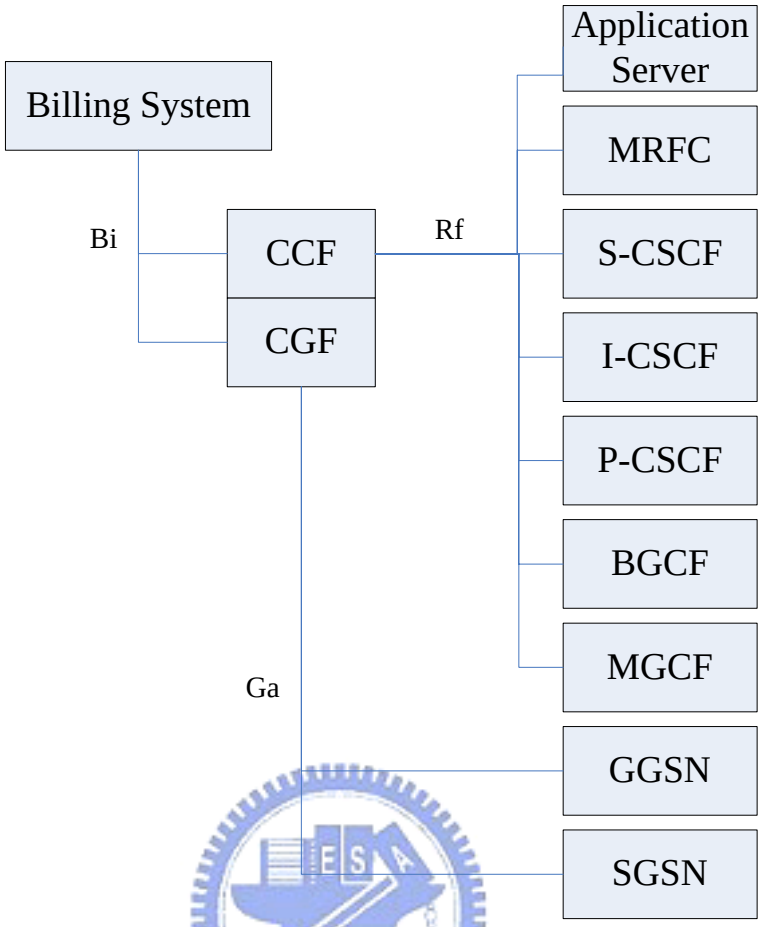

Figure 2-5: Offline IMS charging

Online Charging is an event-based charging between an Application Server (AS) or MRFC and the Event Charging Function (ECF). There are two sub-functions fro Online Charging.

- Immediate Event Charging
  - Decentralized Unit Determination and Centralized Rating
  - Centralized Unit Determination and Centralized Rating
  - Decentralized Unit Determination and Decentralized Rating
- Event Charging with Reservation
  - Decentralized Unit Determination and Centralized Rating
  - Centralized Unit Determination and Centralized Rating
  - Decentralized Unit Determination and Decentralized Rating

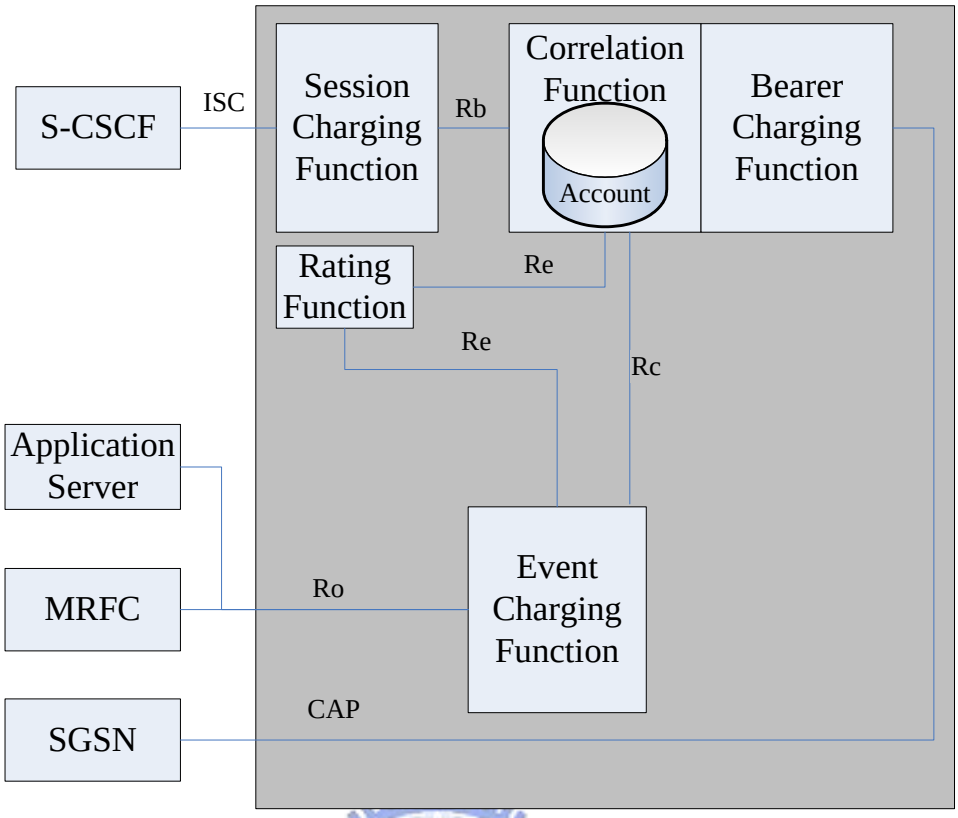

Figure 2-6: Online IMS charging

2.3 Protocols used in Our Solution

2.3.1 Diameter

Diameter [12] The AAA Working Group of the Internet Engineering Task Force (IETF) designed the specification of the AAA (Authentication, Authorization, and Accounting) protocol, Diameter, which is improved from Radius (Remote Access Dial-IN User Service). It provides more secure authentication, authorization and accounting than Radius.

Table 2-1: The command name of Diameter

Command-Name	Function
Abort-Session-Request (ASR), Abort-Session-Answer (ASA)	Send to stop a session by a server and the answer message
Accounting-Request (ACR), Accounting-Answer (ACA)	Send to exchange accounting information with a peer and the answer message.
Capabilities-Exchange-Request (CER), Capabilities-Exchange-Answer (CEA)	Send to exchange local capabilities and the answer message.
Device-Watchdog-Request (DWR), Device-Watchdog-Answer (DWA)	Send to peer when no traffic have been exchanged and the answer message.
Disconnect-Peer-Request (DPR), Disconnect-Peer-Answer (DPA)	Send upon detection of a transport failure and the answer message.
Re-Auth-Request (RAR), Re-Auth-Answer (RAA)	Send to request user be re-authenticated or re-authorized and the answer message.
Session-Termination-Request (STR), Session-Termination-Request (STA)	User send request server to terminate this authenticated session and the answer message.

Diameter is designed to be extensible, defining new AVP values, creating new AVPs, creating new authentication/authorization applications, creating new accounting applications, application authentication procedures. Diameter base protocol provides some basic command, listed in Table 2-1. In the IP Multimedia Subsystem, it define two charging interfaces, Rf and Ro, which is based on Diameter base protocol.

2.3.2 SIP

The Session Initiation Protocol (SIP) [14] is an application control protocol, which provides creation, modification, termination with one or more participants. These sessions include call setup, multimedia conferences and etc. its syntax and semantics are similar to Hypertext Transfer Protocol (HTTP). It can be used in conjunction with several other IETF protocols such as Session Description Protocol (SDP). There are four logical types of entities: user agents, registrar, redirect server and proxy server.

Table 2-2: The request methods of SIP

Message Name	Function
INVITE	Invite use to join a session.
ACK	Acknowledge to an INVETE request
BYE	A call is to be released
REGISTER	Register to a SIP server
CANCEL	Cancel a pending request
OPTIONS	Query the capabilities of a server

In the IMS, SIP is used to be the registration and setup the phone call between use and operation core network.

2.4 Mobile Payment

Mobile Payment may become a major application for mobile devices, it enable the users to perform commercial transactions wherever they are. These services require security and 3G network provide basic access security.

There are four parties involved in a mobile payment transaction. The user and Merchant are the most important roles in the mobile commerce. A User buys goods or downloads contents from the merchants and the behaviors make the requirement of payment. A network operator (mobile payment service provider) and a third party are responsible to provide payment service. A network operator can sign a contract with the third parties. A network operator provides the user's authentication to the third parties. They provide the secure payment methods to users. Their relationships are shown in Figure 2-7.

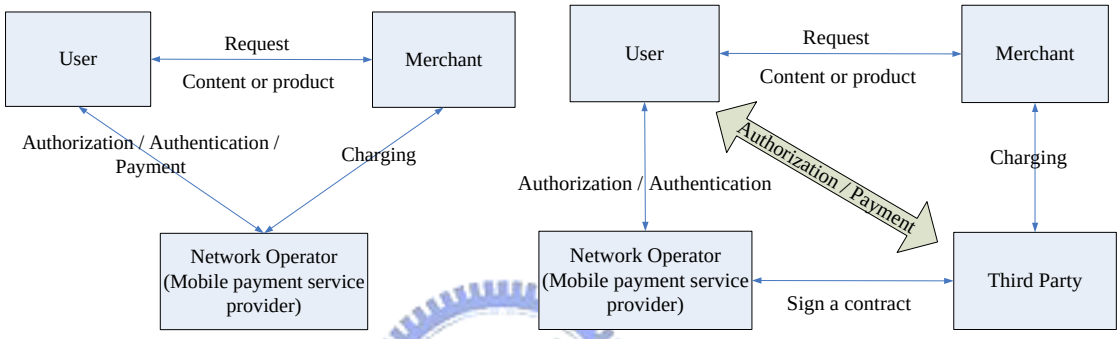

Figure 2-7: The relationship of the mobile payment entities

In 3G Networks, the network operators should promote themselves to be the Mobile Payment Service Provider. They also can cooperator with other third-party in the strategic alliance. We will introduce some mobile payment systems in next section.

2.4.1 Sonera

Sonera is a Telecom company in Finland. Sonera MoiblePay is an operator-independent mobile payment scheme. After registering with the system, user's payment accounts are debited directly from his bank account or charged to a credit card. The mobile user calls a special number, which is equal to a vendor-specific machine. Merchant can pay the cost of this call for this transaction. This call is routed to the MobilePay server and user can be identified using the caller identification feature of GSM. If a user calls a phone number of vending machine, he can input a fixed number associated with each good. Purchase money

with each fixed number is debited from the user's account at this server. The server can request a PIN from the user to confirm this transaction. The MobilePay Server then sends the notification by making another GSM call to the merchant mobile device in this vending machine and good can be released. The procedure is shown in Figure 2-8.

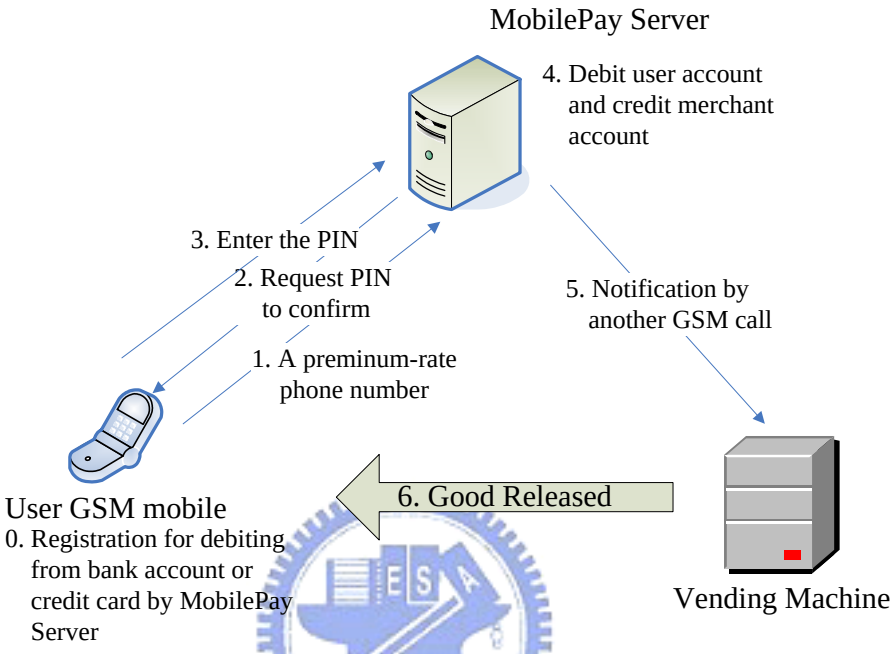

Figure 2-8: Sonera MobilePay

2.4.2 GiSMo

GiSMo is a subsidiary of Millicom International Cellular, a wireless carrier and operator of cellular networks around the world, with headquarters in Sweden. To use the system, a customer must open a GiSMo account; it may link to an existing bank account or credit card. This GiSMo account also links to the user's mobile phone number for the purchase authorizations. The steps about these transactions are shown in Figure 4-2. The server creates a random transaction code and sends this to the user's GSM mobile phone by using SMS. The user must reenter the code obtained on his phone into another Web form on his Internet computer. Then the code is sent back to the GiSMo Server. If the code is correct, the server

will return acknowledges to the user and merchant. Then server debit or credit their accounts. The procedure is shown in Figure 2-9.

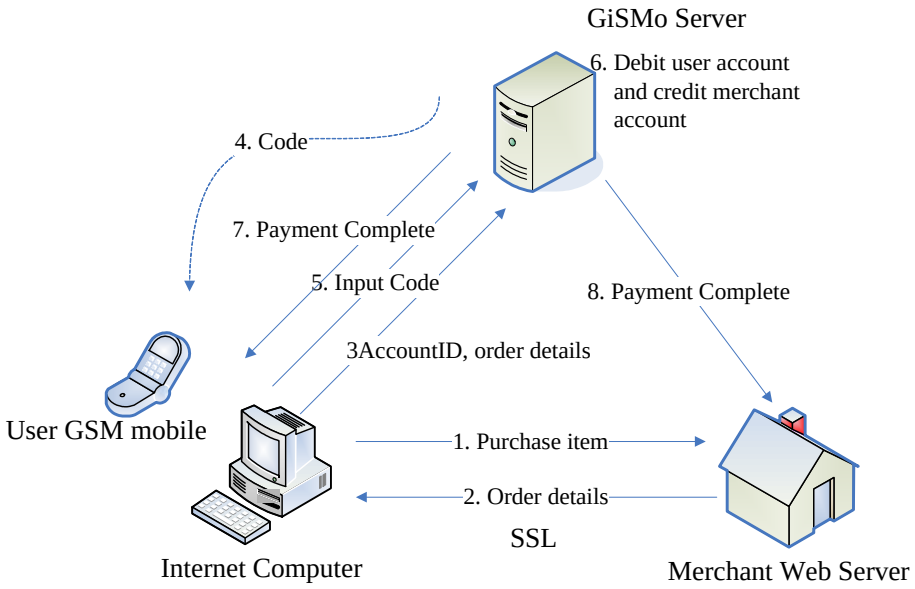

Figure 2-9: GiSMo Internet purchase

2.4.3 Paybox

Paybox [1] is an operator-independent mobile service provider. Paybox where Deutsche Bank owns a 50% stake runs the first payments commencing in Germany in May 2000. Paybox has been initially targeted at GSM users and use user's phone number as the identity. The merchants and users must exchange mobile phone number first. The user informs the merchant of his or her mobile phone number to initiate a payment. In mobile network, the user can call the merchant GSM phone number. For physical world, the user passes the number to the merchant. And in the internet, user enters phone number into a web form, and sent securely over SSL to the merchant web server. Then user purchases in the merchant store or web site. The merchant sends the total amount of the payment to Paybox server by a toll-free number from merchant's mobile phone. Paybox server notify user the total amount of payment by another GSM call and the user input the PIN to confirm this transaction. Paybox

server notifies the merchant of the result and debit user account and credit merchant account. The procedure is shown in Figure 2-10

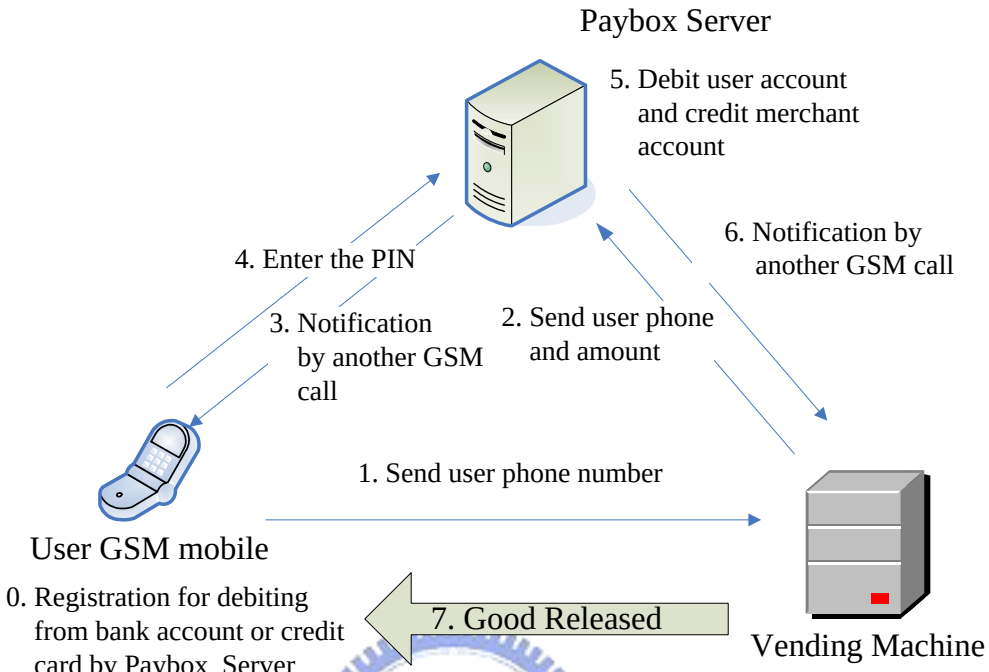

Figure 2-10: Paybox

Chapter 3 Solutions for Anonymous Mobile Payment

In this chapter, we have proposed an approach to support anonymous mobile payment through 3G network operators. In our proposed solution, we reuse the 3G security architecture to authenticate the users who can use the anonymous mobile payment service. In addition, we add new anonymous feature in this service and the users can use the prepaid account, postpaid account or third party account to pay the payment.

First, we will describe the mobile payment landscape and basic assumptions in our approach. The proposed anonymous mobile payment solutions will be explained later.

3.1 The Basic Assumptions and Mobile Payment Landscape

The future mobile payment landscape is a telecommunication network that consists of multiple mobile devices, network operators and many values-added service providers, such as a 3G IP network. Figure 3-1 depicts the variety of telecommunication networks. Multiple mobile devices, network operators and service providers are connected together with wireless or wired networks.

We use the mobile devices equipped the SIM/USIM card under a single telecomm network operator, such as Chunghwa Telecomm Co. (CHT) and Taiwan Cellular Corp. (TCC). Different network operators are connected together. They provide mobile payment services. There are also all kind of value-added service providers which may be virtual or physical stores and provide all kinds of services to users. They may sign contracts with the network

operators to cooperator with each other for gaining more profit or sharing risks. Anonymous mobile payment is a process of finance. A brief description of mobile payment flow is given in the next section.

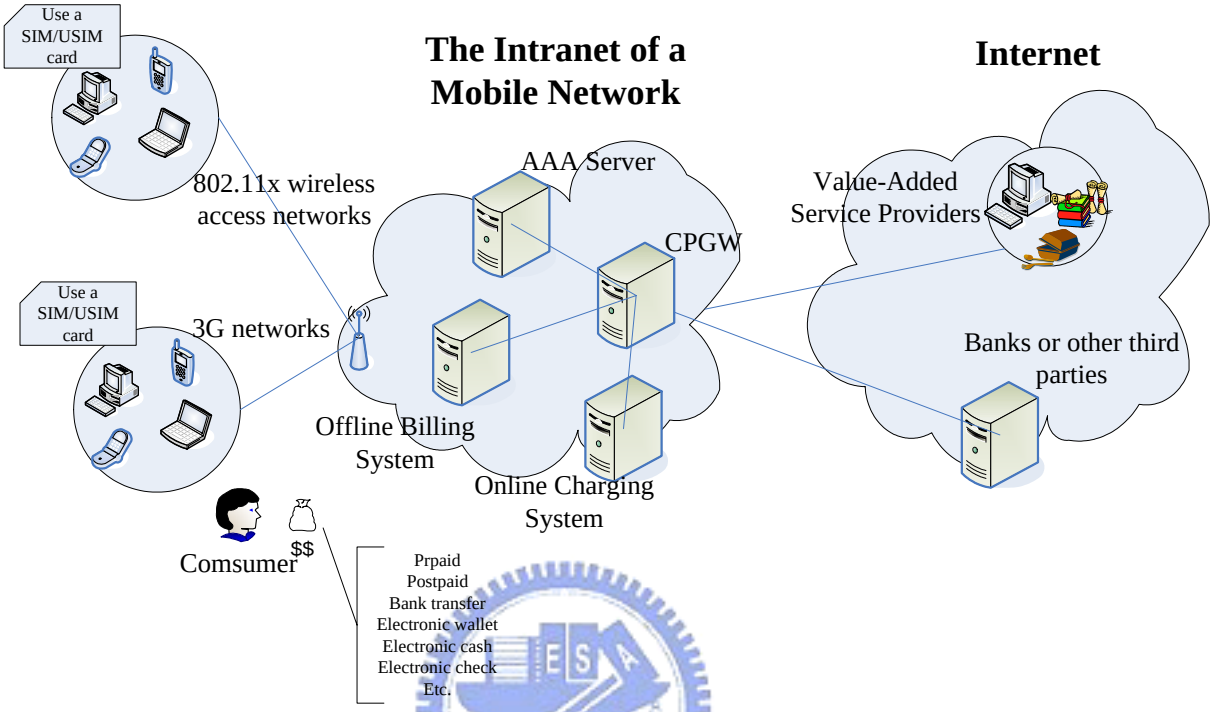

Figure 3-1: The scenario of the future mobile payment landscape

3.1.1 A Payment Service Provider

In the Internet, there are already many payment models, including prepaid card, small payment which is proposal by telecommunication network operator, electronic wallet, electronic cash, electronic check, etc. But these payment models described above will not satisfy various situations anymore, such as the users can choose by themselves which payment accounts they pay to the merchant, in the mobile networks of the future. We need a new mobile payment solution as we will describe later.

In mobile payment, we also need payment service provider. We can usually see three kinds of providers, bank, credit card company and mobile network operator which is the newest coming payment service provider. We compare them in Table 3-1 [4].

Table 3-1: Payment Service Providers

Items	Bank	Credit Card Company (VISA, MASTER and etc.)	Mobile Network Operator
The ability of providing financial service	Good	Good	Bad
The ability of providing mobile service	Bad	Bad	Good
The ability of authentication	Normal	Normal	Good
The ability of controlling risks	Normal	Normal	Bad
The number of customers	Normal	Many	Fewer
The merchants with signing the contract	Normal	Many	Fewer

One advantage of a mobile payment system administered by a network operator is that payments can be charged directly to the subscriber's phone bill. We focus the payment service as the extension of the network operator.

3.1.2 Basic Assumptions

The future mobility landscape is an all-IP network including wireless access networks and wired IP backbone.

The assumptions that we explicitly make in the thesis are listed below:

1. The mobile station equipped SIM/USIM card is authenticated by network operator.
2. We follow the 3GPP specification charging principles and focus on choosing payment account to the payment by the users themselves.
3. We suppose the same 3G authentication mechanism can be reused for the mobile payment service.

4. We keep the user privacy in the network operator and the network operator won't leak user privacy to the merchant if user doesn't allow.
5. We use mobile devices equipped with a USIM/SIM card and SIP UA application.
6. The mobility will handle by radio wireless technologies, such as W-CDMA, TMDA, and WLAN 802.11 etc.
7. We do not handle shopping protocol; we provide the payment information such as provisional identity described in the next section to shopping protocol.
8. The Charging/Payment Gateway can be enhanced to credit or debit the prepaid and postpaid account.

3.2 Proposed Solution Architecture for the Network Operators

3.2.1 Anonymity

People can have a certain level of anonymity in the real life. They do not have to reveal their identity in many situations. For example, someone can buy a movie ticket with cash and you can see the movie anonymously with many people. Because he gets a valid ticket which is authorized to the movie theater; he does not reveal his identity.

In the virtual world, people can buy what they need without face to face contact through the internet, telephone, fax or postal parcel. It is strongly based on authentication and authorization in electronic transactions. It usually uses user name, phone number, or account registered in the merchant authentication to distinguish name of entity to authorize these electronic transactions. In some cases, it is not necessary that the entity should provide their name or some information to another entity for the transactions such as content downloading.

Anonymity, privacy and security are related. There are many reasons to hide your identity when you do the mobile payment. If you can anonymously pay, you can keep your privacy. You need a security technique to protect in the virtual world from catching your information or assuming your identity by others.

3.2.2 Anonymous Mobile Payment

In the real world, we can be sure of the complete anonymous payment on purchase by paying cash. But in the electronic transactions, we will leave our transaction records including session record, access record and any other record that we may want to keep. In the electronic mobile payment, we can get certain level anonymity if we can completely trust our network operator to keep our privacy.

In our solution, we provide provisional identity instead of permanent identity like telephone number or user name. This provisional identity is generated randomly and different in every transaction if a user registers payment service again. Every transaction with the provisional identity is also recorded. Merchants can not find regular information about user from the provisional identities if users do not want to let them acquire the information.

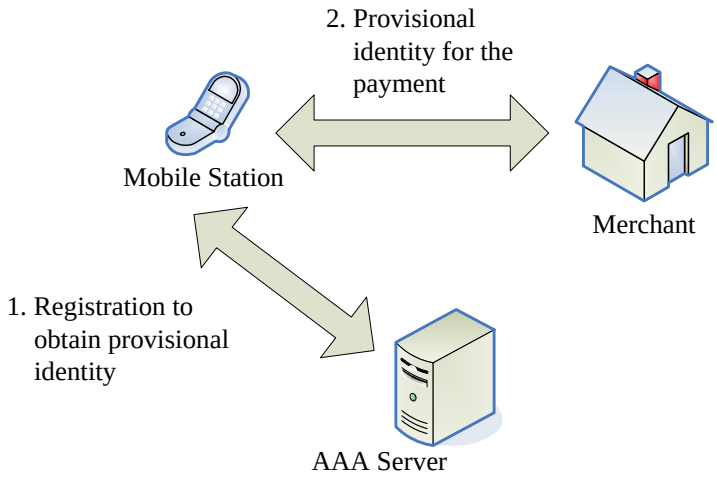

Figure 3-2: Anonymity by using provisional identity

3.2.3 The Proposed Solution Architecture

Figure 3-3 depicts our proposed architecture. The function of each component is described below.

1. AAA server and AAA DB: An AAA server and DB are responsible for the authentication, authorization and accounting to users in the network operators. All users should send a registration request message to the AAA server when they want to use anonymous mobile payment service. The AAA server maintains the registration information of the users and checks the users' privilege of using payment service. The AAA DB stores the user profile.
2. Home Subscriber Server (HSS): HSS is a database the store the users profile in 3G network. It provides functions include the Home Location Register (HLR), DNS, security databases. And new functions for the Internet type protocols are also included such as Diameter or ipv4/ipv6 capability.
3. GPRS Support Node (GSN): GSN provides the interface of using wireless network resource and connect to the Public Domain Network (PDN).
4. Charging/Payment Gateway: Charging/Payment Gateway can process the payment from prepaid, postpaid or transferring accounts to the bank; it depends on the user's decision.
5. Charging Gateway Function: CGF process the charging information from the GSNs and transfer the collection information to the network operator's Billing System. CGF may be supported as a centralized separate network or as a distributed functionality in the GSNs.
6. Banks or other third parties: They are also the finance house. They provide different payment solutions to users. The network operators can cooperate with them.
7. Billing System: Billing System is designed to support the business models, such as postpaid, prepaid. It can use multiple rates to satisfy users and gather the statistics of users' habits.

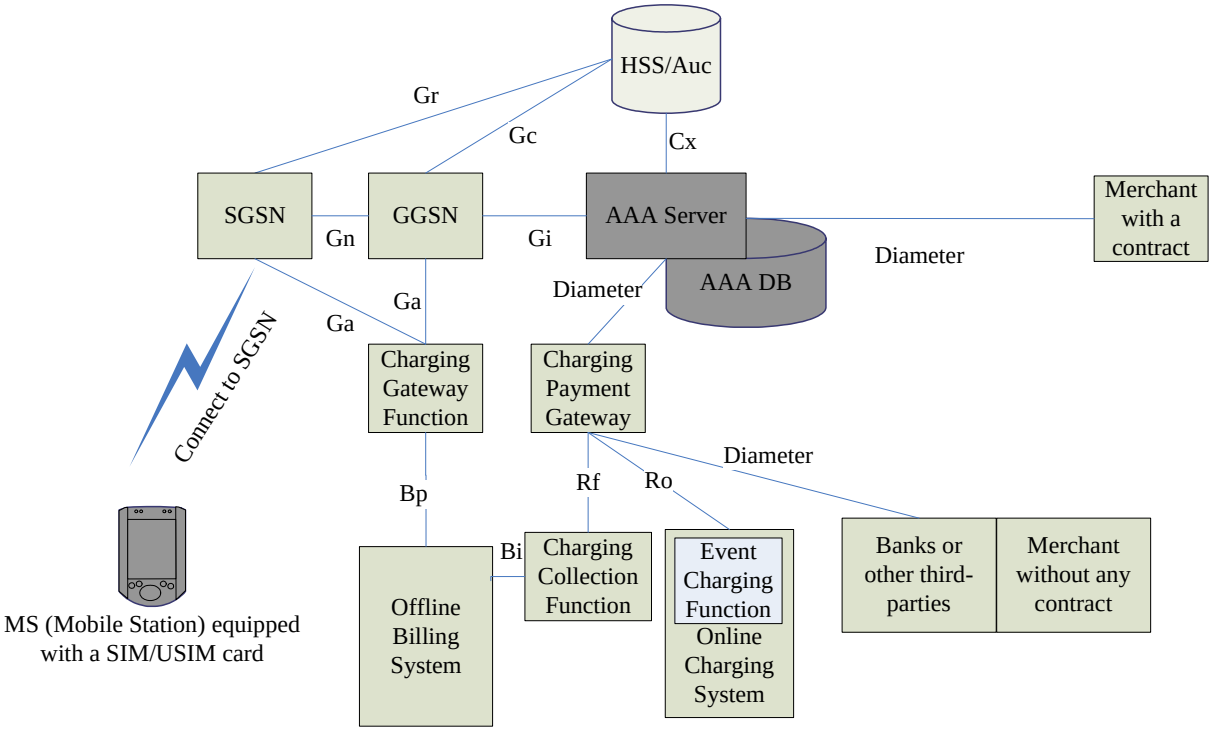

Figure 3-3: Proposed solution architecture

3.2.4 Authentication for the Payment Service

After performing Packet Data Protocol (PDP) context activation to obtain access privilege to the GPRS network, the MS can request the payment services through the registration procedure as the Figure 3-4 showing. It is shown in Figure 3-5 how the authentication vectors and other parameters such as RAND, AUTH and RES are produced [11, 14].

Registration procedure:

1. The MS sends a SIP Register message including IMPI to the AAA server.
2. The AAA server invokes the authentication vector procedure by sending Cx [13] MAR message to HSS.
3. The HSS response with an AV array to the AAA server.
4. The AAA server selects an unused AV and sends the parameters RAND and AUTN to the

MS.

5. The MS checks whether the received AUTN whether it can be accepted. Then produces a response RES to the AAA server.

6. The AAA server sends a 200 OK message with provisional identity to the MS, the payment service registration procedure completes.

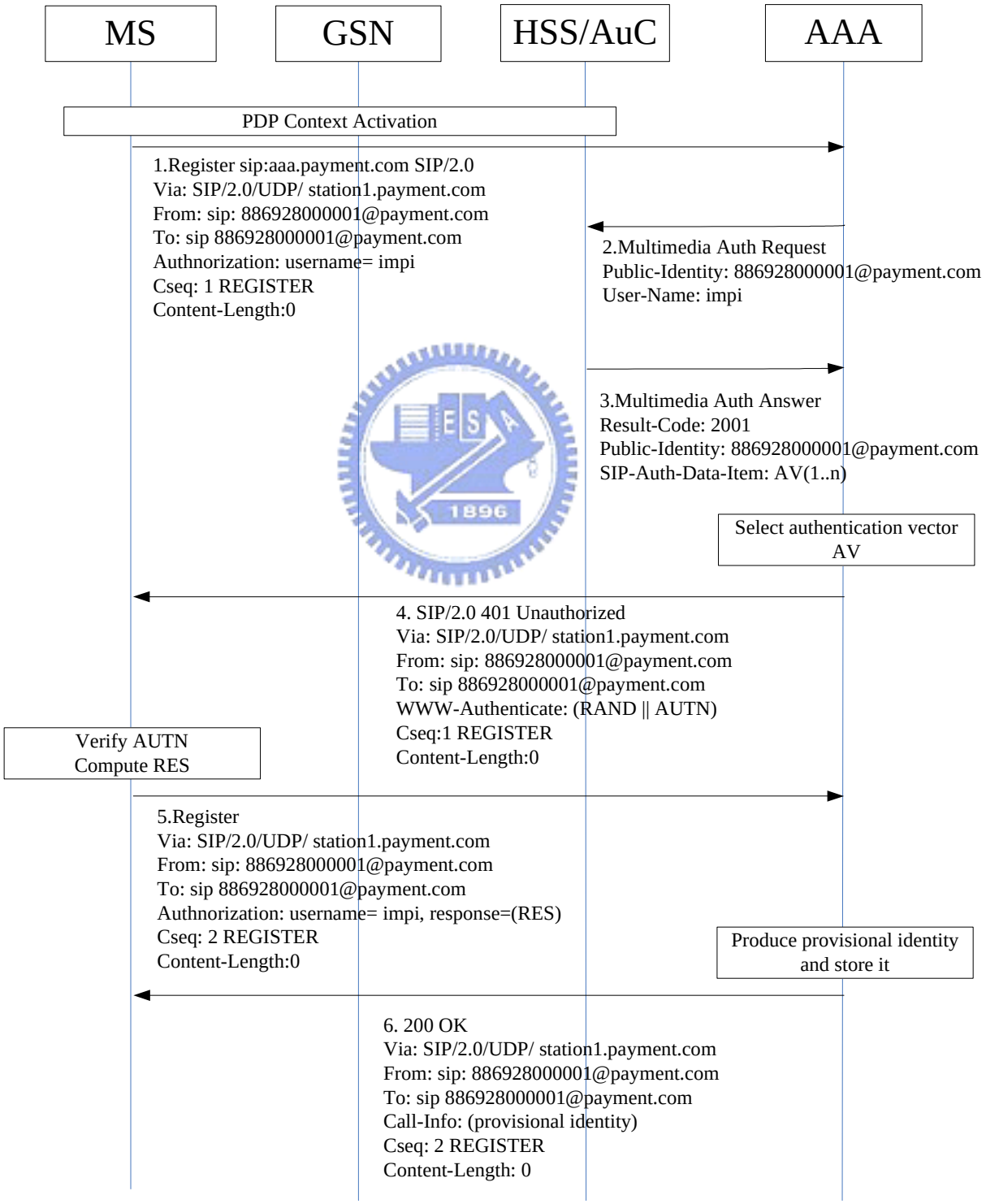

Figure 3-4: Payment service registration procedure (SIP/SIM-based authentication)

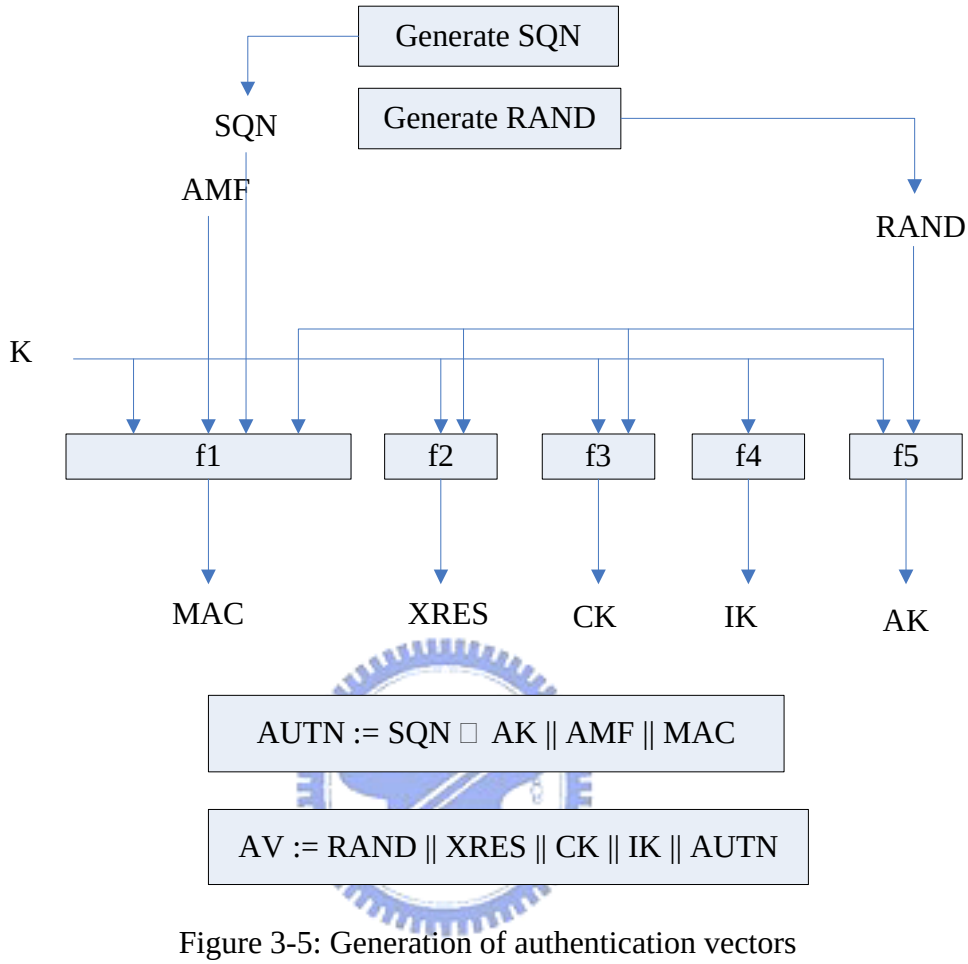

Figure 3-5: Generation of authentication vectors

3.2.5 Operations for the Anonymous Mobile Payment

We can probably define three scenarios to the mobile payment. The most mobile payment scenario the users may use is in the same networks. We also use mobile device to pay through the internet or we can pay through the third party. The merchant may provide any services such as content web site, book store etc. The MS may be any mobile device equipped with a SIM/USIM card.

We can use the two commands, Accounting Request and Account Answer, defined in Diameter base protocol and shown in Tables 3-2 and 3-3. Also, we define new AVPs to

support our proposed solution. Merchant-Name is used to record the merchant name the user wants to pay. Request-Account-Action is used to assure which payment methods the users want to pay. 0: prepaid, 1: postpaid, 2:bank transfer, 3: thirdparty and 4: request payment code. Payment-Code is used to record the payment code. Service-Unit is used to record the unit that the users want to pay. Accounting-Record-Type had been defined in Diameter base protocol. 1: ENENT_RECORD, 2: START_RECORD, 3: INTERIM_RECORD and 4: STOP_RECORD.

Table 3-2: Diameter AVPs for Accounting-Request command

Attribute Name	**Code**	**Value Type**
Session-Id	263	UTF8String
Origin-Host	264	DiamIdent
Origin-Realm	296	DiamIdent
Destination-Realm	283	DiamIdent
Accounting-Record-Type	480	Enumerated
Accounting-Record-Number	485	Unsigned32
Acct-Application-Id	259	Unsigned32
Vendor-Specific-Application-Id	260	Grouped
User-Name	1	UTF8String
Accounting-Sub-Session-Id	287	Unsigned64
Accounting-Session-Id	44	OctetString
Acct-Multi-Session-Id	50	UTF8String
Acct-Interim-Interval	85	Unsigned32
Accounting-Realtime-Required	483	Enumerated
Origin-State-Id	278	Unsigned32
Event-Timestamp	55	Time
AVP		
Proxy-Info	284	Grouped
Route-Record	282	DiamIdent
New Attributes Defined for Mobile Payment		
Service-Unit		Grouped
Merchant-Name		UTF8String
Request-Account-Action		Enumerated
Payment-Code		UTF8String

Table 3-3: Diameter AVPs for Accounting-Answer command

Attribute Name	Code	Value Type
Session-Id	263	UTF8String
Result-Code	268	Unsigned32
Origin-Host	264	DiamIdent
Origin-Realm	296	DiamIdent
Accounting-Record-Type	480	Enumerated
Accounting-Record-Number	485	Unsigned32
Acct-Application-Id	259	Unsigned32
Vendor-Specific-Application-Id	260	Grouped
User-Name	1	UTF8String
Accounting-Sub-Session-Id	287	Unsigned64
Accounting-Session-Id	44	OctetString
Error-Reporting-Host	294	DiamIdent
Acct-Interim-Interval	85	Unsigned32
Accounting-Realtime-Required	483	Enumerated
Origin-State-Id	278	Unsigned32
Event-Timestamp	55	Time
AVP		
Proxy-Info	284	Grouped
New Attributes Defined for Mobile Payment		
Payment-Code		UTF8String

3.2.5.1 Payment flow in home network

This section illustrated the operations of user and merchant are in the same home network. There are two kinds of operations in this scenario. One is “Registration” operation which has been described in section 3.2.4 and the other is “Payment” operation. We use the message flow to describe the inter-working of each network components. Message exchange is based on the scenario discussed above.

Payment operation: After a MS completes the registration operation.

1. When the user decides to purchase or download the content from the merchant, he or she

uses the MS to send an Account Request message with the user's, merchant's and payment information to the AAA server.

2. The AAA Server checks a user's permission whether the MS has the privilege to use the payment service. If a user uses prepaid account, there is a need to check user account. The detail will be described in session 3.2.6.1.
3. Assume that the user passes the authorization from the AAA server. The AAA server sends an Account Request message to merchant. Merchant checks the transaction.
4. The Merchant replies the result of Account Answer message to the AAA server.
5. The AAA server replies the result of Account Answer message to the MS.
6. Assume that the transaction successes. The AAA server sends an Account Request message with the transaction information to the CPGW.
7. The CPGW issues a fund transfer by payment method. The detail will be described in session 3.2.6.
8. The CPGW replies the result of Account Answer message to the AAA server.

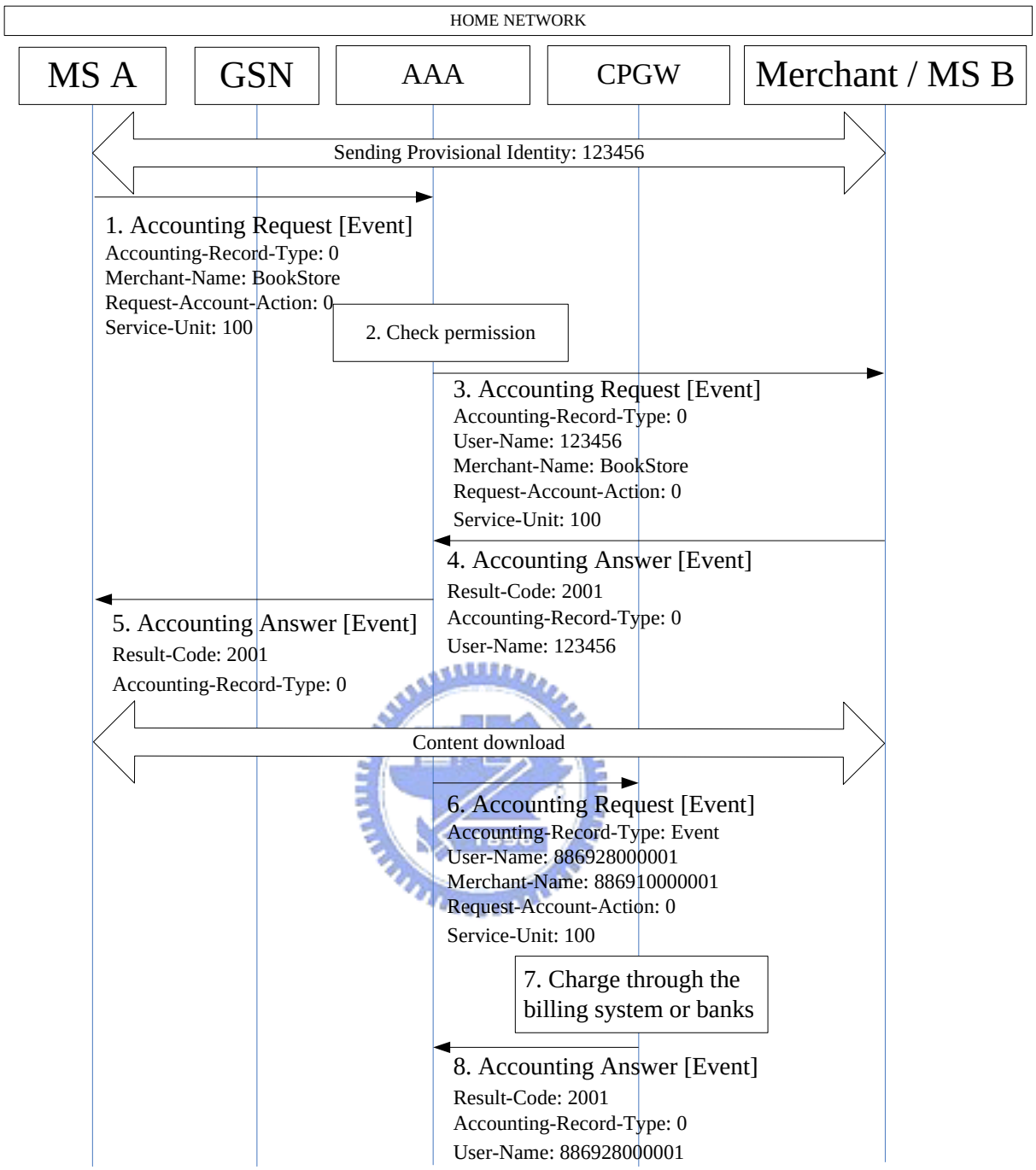

Figure 3-6: Payment flow in home network

3.2.5.2 Payment flow by using payment code

We can purchase from internet, it is just like that we use a PC and make the ecommerce in the internet. Because the merchants in the Internet or other visited Networks can not been authenticated by the network operator, we provide a method of payment code to support the

need of these users. The method can also to support movie ticket system. The network operators can cooperator with a movie theater to reserve tickets for the users and the users can get the payment code as the tickets and pass quickly through a verification machine.

Payment operation: After a MS completes the registration operation.

1. When the user decides to purchase or download content from merchant, he or she uses a MS to send an Account Request with user's information to request payment code to the AAA server.
2. The AAA server checks user's permission whether MS has the privilege to use the payment service.
3. Assume that user passes the authorization from the AAA Server. The AAA server replies an Account Answer message with a payment code.
4. The user inputs the payment code through his or her browser of the MS to the merchant.
5. The Merchant replies the result to the MS.
6. Assume that the Merchant accepts the payment code. The Merchant sends an Account Request message with payment code.
7. The AAA server checks the code whether it is valid.
8. The AAA server replies the result of Account Answer message to merchant.
9. Assume that the transaction successes. The AAA server sends an Account Request message with the transaction information.
10. The CPGW issues a financial transfer by payment method.
11. The CPGW replies the result of Account Answer message to the AAA server.

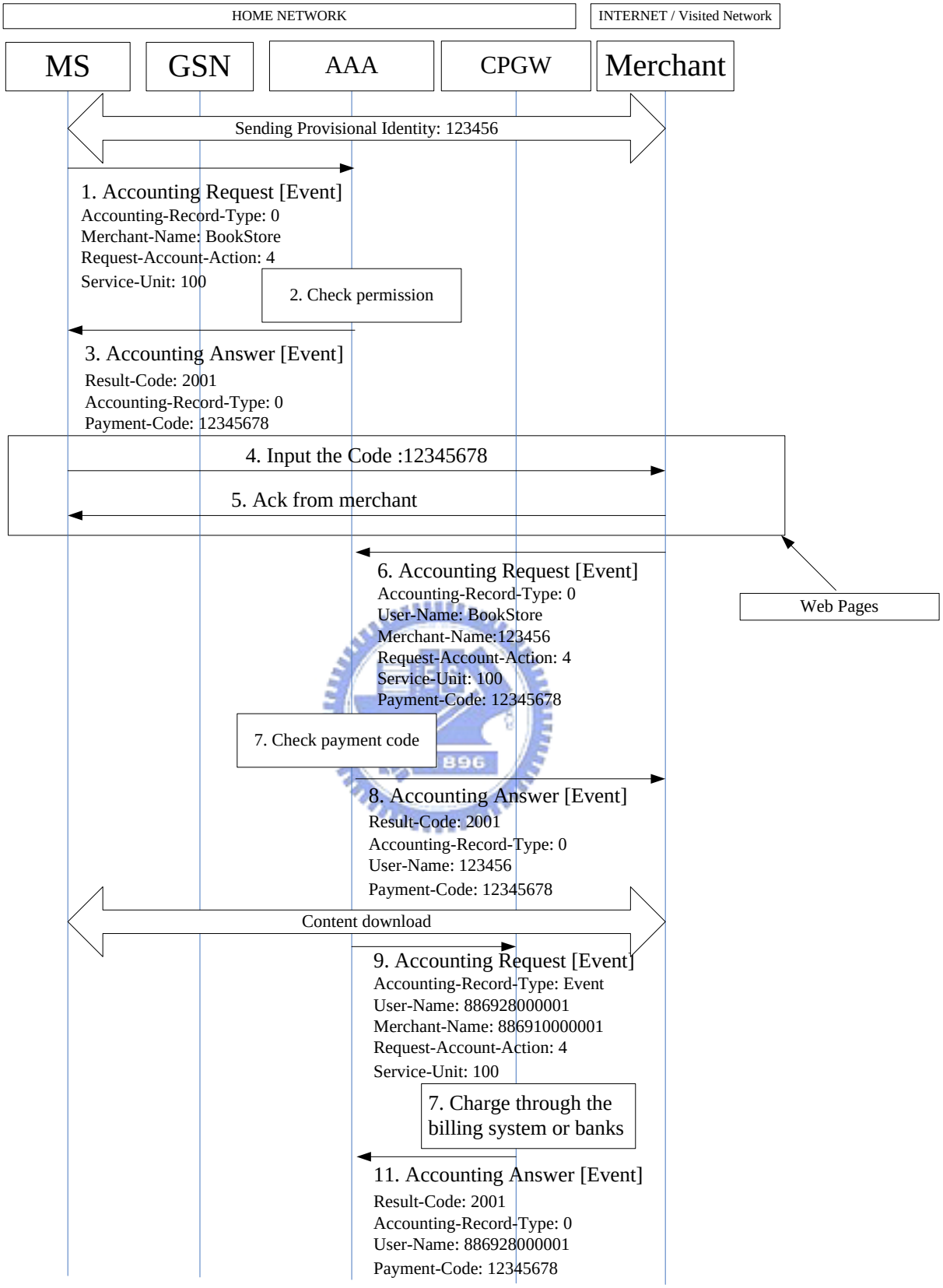

Figure 3-7: Payment flow by using payment code

3.2.6 Operations for the CPGW

The Charging/Payment Gateway (CPGW) is responsible for account transfer to the financial companies. In our assumption described in section 3.1.2, the CPGW should be enhanced to credit or debit the prepaid and postpaid account of the users and it also can exchange the payment transaction messages with third parties, such as banks.

Online charging and offline charging are be defined to support prepaid and postpaid service. Thus there is a need to cooperate between CPGW and Event Charging Function (ECF). The ECF is charging function for the online charging system. There is also a need to cooperate between CPGW and Charging Collection Function (CCF). The CCF is charging function for the offline billing system. CCF can transfer the Payment CDR of postpaid service. CPGW should have to develop with Rf and Ro [5] interface to support prepaid and postpaid service. We use the Diameter as to transfer protocol to transfer the payment message between CPGW and the third parties.

For our need, we should add addition record type for the postpaid service. In 3GPP specification, the CCF is responsible to produce S-CSCF-CDR, I-CSCF-CDR, P-CSCF-CDR, BGCF-CDR, MGCF-CDR and AS-CDR. We need to add a new record type, Payment CDR, for our proposed mobile payment service. We use Record Type and Service Specific Data field to record our payment CDR. And the AVP Requested-Service-Unit with negative value of Accounting Request between the CPGW and CCF or ECF means that the user's payment will be credited to the merchant account.

Table 3-4: An example of Charging Data of IMS CDR Types

Field	CDR Type
Record Type	Payment CDR
Node Address	127.0.0.1
Session ID	1111111
Calling Party Address	886928000001
Called Party Address	886810000001
Service Request Time Stamp	5/29/2004 10:04 PM
Record Opening Time	5/29/2004 10:05 PM
Record Closure Time	5/29/2004 10:06 PM
Local Record Sequence Number	1
Service Specific Data	Service-Unit:100

Thus a user can make a payment through these payment accounts and choose which account they want to pay. The relationship is shown in Figure 3-8.

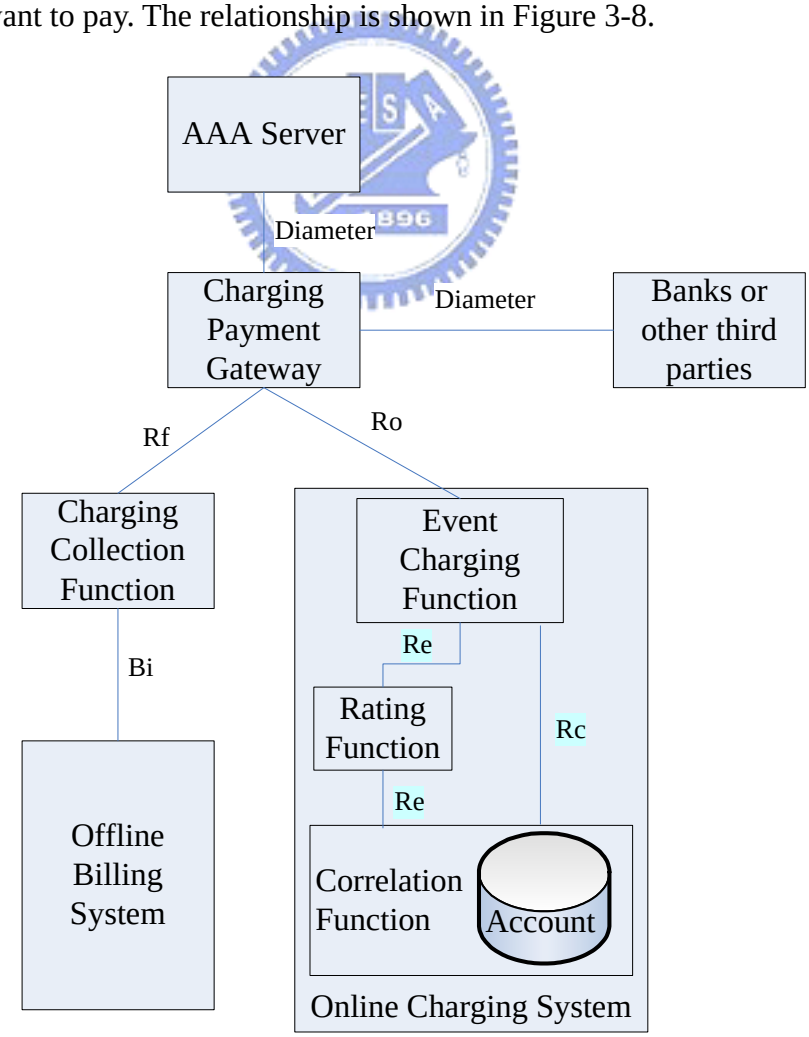

Figure 3-8: Operations for the Charging/Payment Gateway (CPGW)

3.2.6.1 Payment flow for prepaid account query

If a user want to make a payment through his or her prepaid account, it is necessary to check his or her prepaid account first. 3G Online charging provider the Reserve Units and Debit Units Operations described in session 2.2.6. We can use the property to query the user's prepaid account. The procedure is shown in Figure 3-9.

1. When the AAA server sends the Accounting Request message to the CPGW. The AVPs of User-Name and Merchant-Name filled the user's prepaid account are used to indicate the prepaid account query.
2. The CPGW sends Account Request message to the ECF. The AVP of Accounting-Record-Type is set Start.
3. After the ECF performs event charging control to the 3G online charging system, the ECF replies the result of Account Answer message to the CPGW.
4. If the CPGW check the user's prepaid is enough for the payment, it sends the Account Request message with AVP of Account-Record-Type set Stop and AVP Used-Service-Unit set 0 to the ECF.
5. After the ECF performs event charging control to the 3G online charging system, the ECF replies the result to the CPGW.
6. The CPGW replies the result to the AAA server.

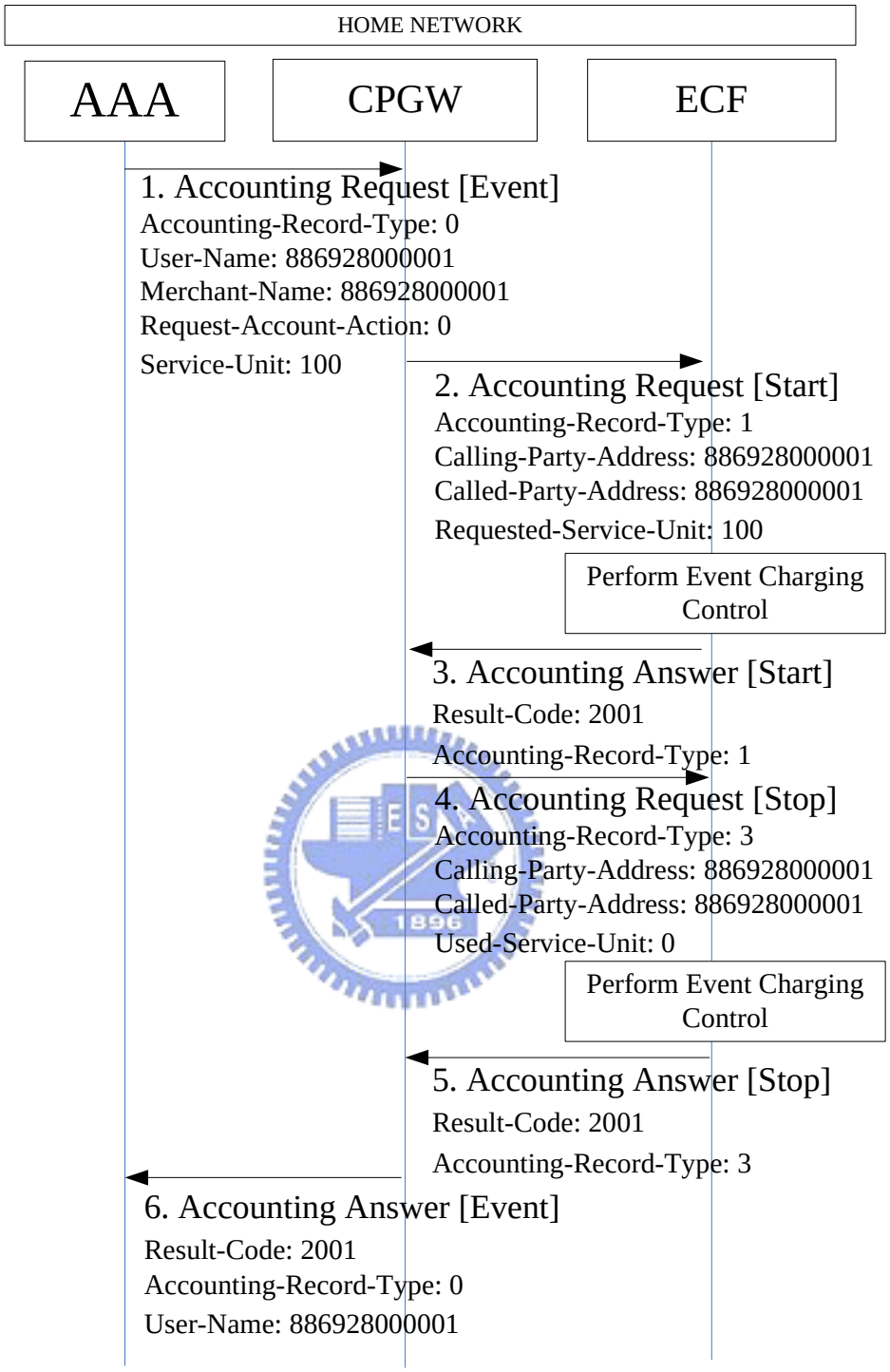

Figure 3-9: Prepaid account query

3.2.6.2 Payment flow for prepaid to prepaid account

If a user wants to transfer his or her prepaid account to the merchant prepaid account, the

operations between the CPGW and 3G online charging system are described in Figure 3-10.

1. The AAA server sends the CPGW an Accounting Request message indicating prepaid account transfer, the account information and the service unit.
2. The CPGW sends the Accounting Request message to the ECF to debit the service unit, 100, in this example, from the user's prepaid account. The AVPs of Requested-Action is set DIRECT_DEBITING and Request-Service-Unit is set positive value.
3. After the ECF performs event charging control to the 3G online charging system and debits the user's prepaid account, the ECF sends the result to the CPGW.
4. The CPGW sends an Accounting Request message to the ECF. The AVPs of Requested-Action is set REFUND_ACCOUNT and Request-Service-Unit is set positive value. Note that the value of Request-Service-Unit is 100 to increase the merchant's credit in his account.
5. After the ECF performs event charging control to the 3G online charging system and credits the merchant's prepaid account, the ECF sends the result to the CPGW.
6. The CPGW sends the result to the AAA server.

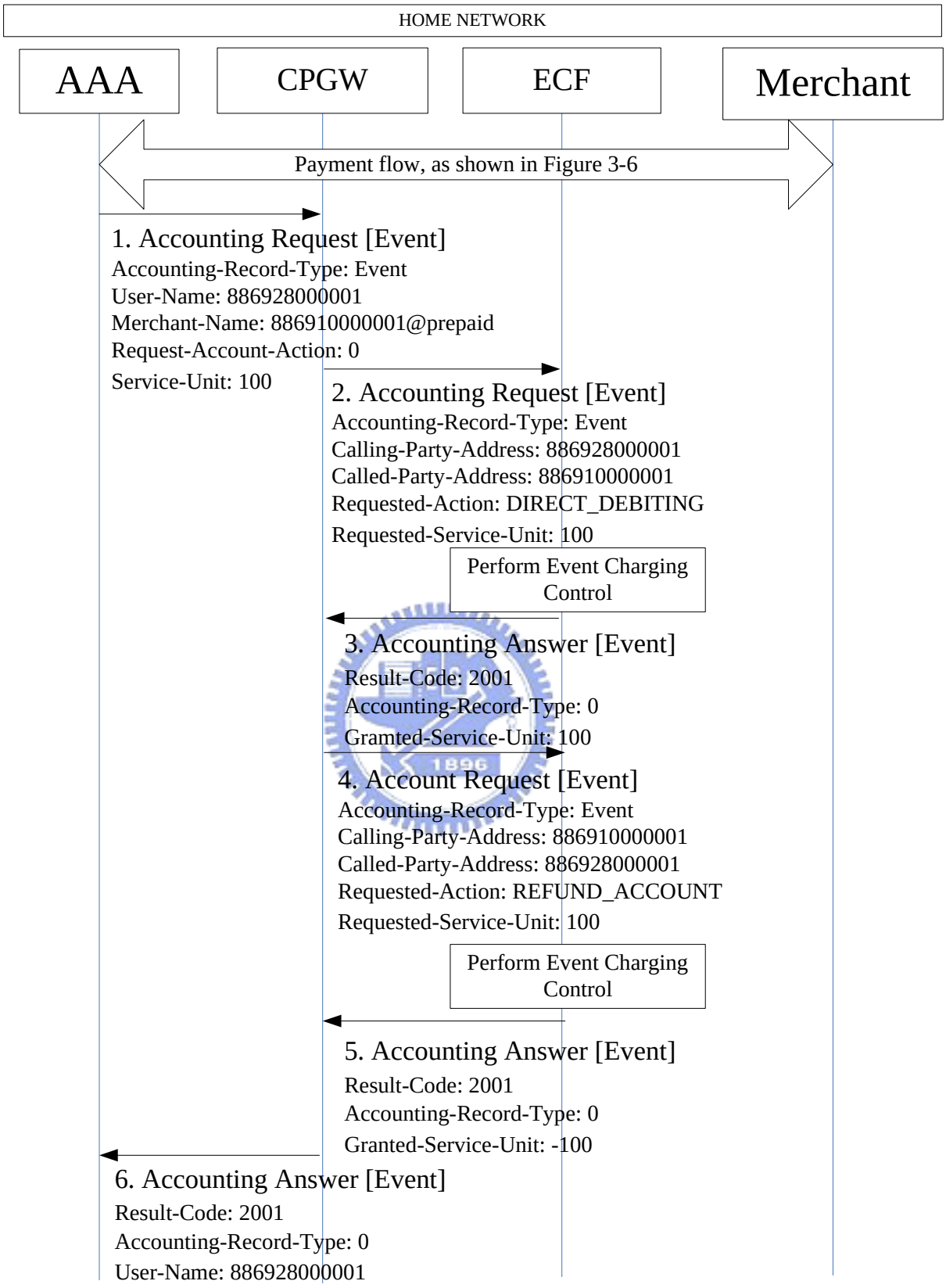

Figure 3-10: Payment flow for prepaid to prepaid account

3.2.6.3 Payment flow for postpaid to postpaid account

If a user wants to transfer his or her postpaid account to the merchant postpaid account, the operations between the CPGW and 3G offline billing system are described in Figure 3-10.

1. The AAA server sends the Accounting Request message to the CPGW with postpaid account debit and credit.
2. The CPGW sends the Accounting Request message to the CCF. The AVP of Request-Service-Unit is set positive value.
3. After the CCF performs event charging control to the 3G offline billing system and creates a Payment CDR of payer, the CCF replies the result to the CPGW.
4. The CPGW sends the Accounting Request message to the CCF. The AVP of Request-Service-Unit is set negative value.
5. After the CCF performs event charging control to the offline billing system and creates a Payment CDR of payee, the CCF replies the result to the CPGW.
6. The CPGW replies the result to the AAA server.

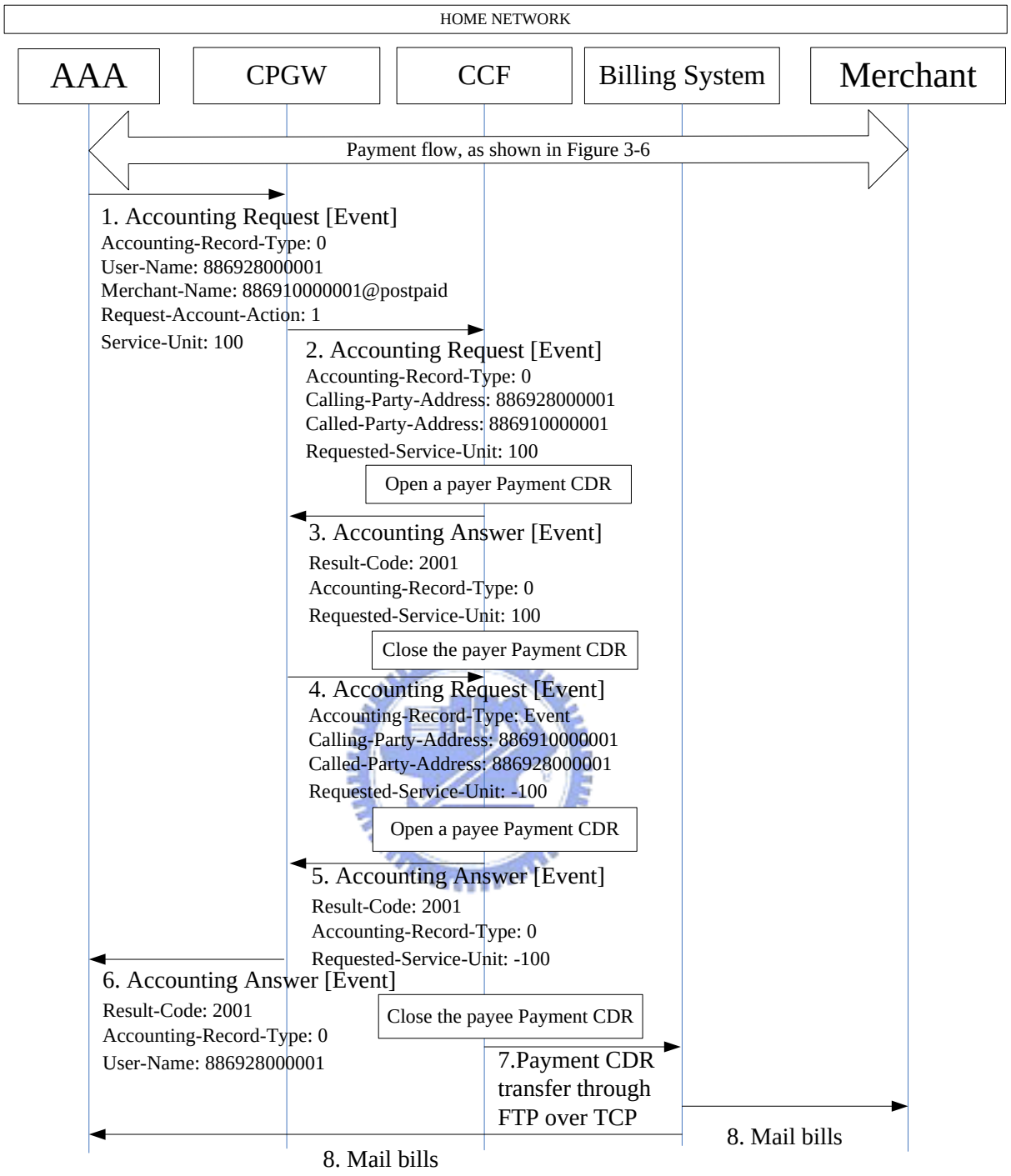

Figure 3-11: Payment flow for postpaid to postpaid account

3.2.6.4 Payment flow for third party to third party account

The procedure is similar with as above we had described and shown in Figure 3-12.

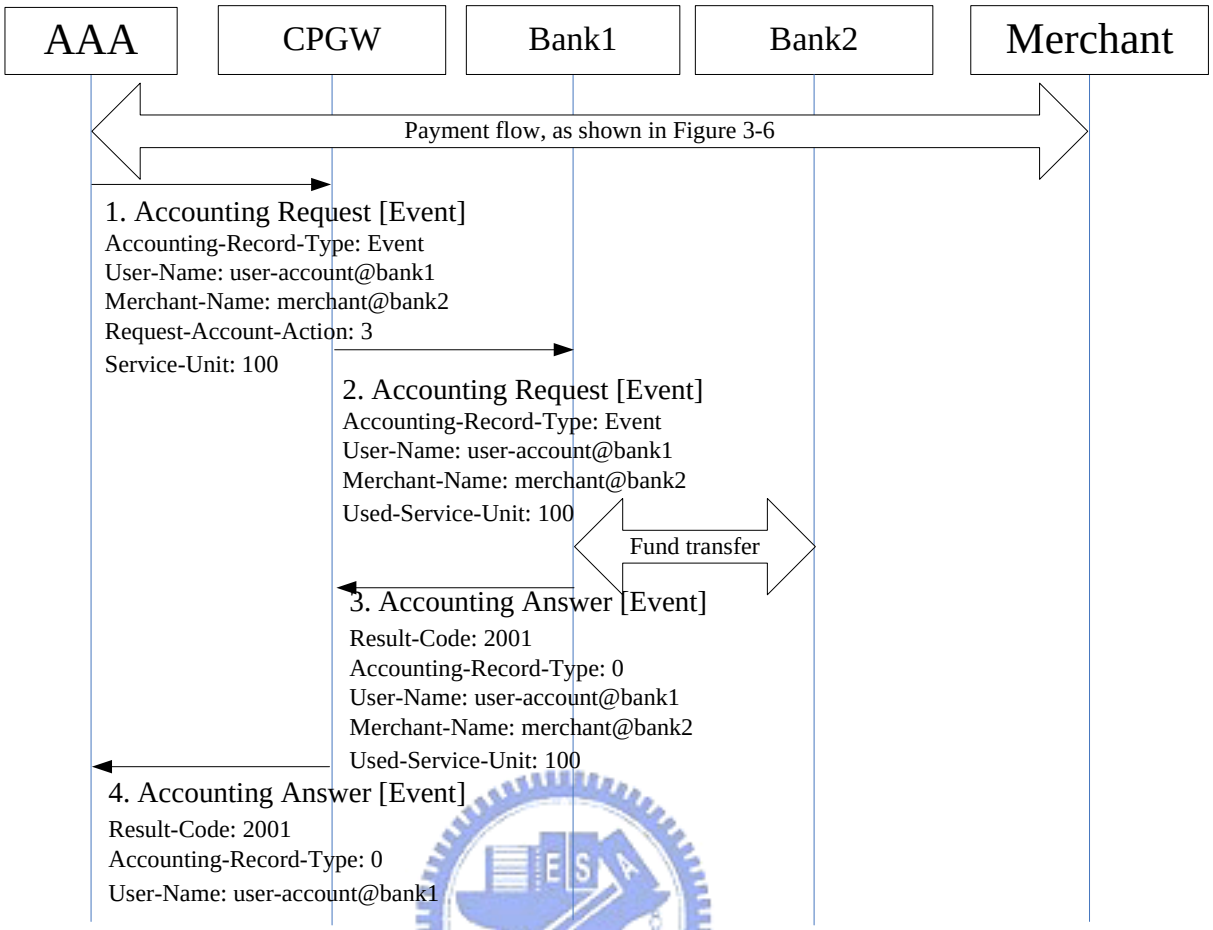

Figure 3-12: Payment flow for third party to third party account

3.2.6.5 Payment flow for postpaid to third party account

The procedure is similar with as above we had described and shown in Figure 3-13.

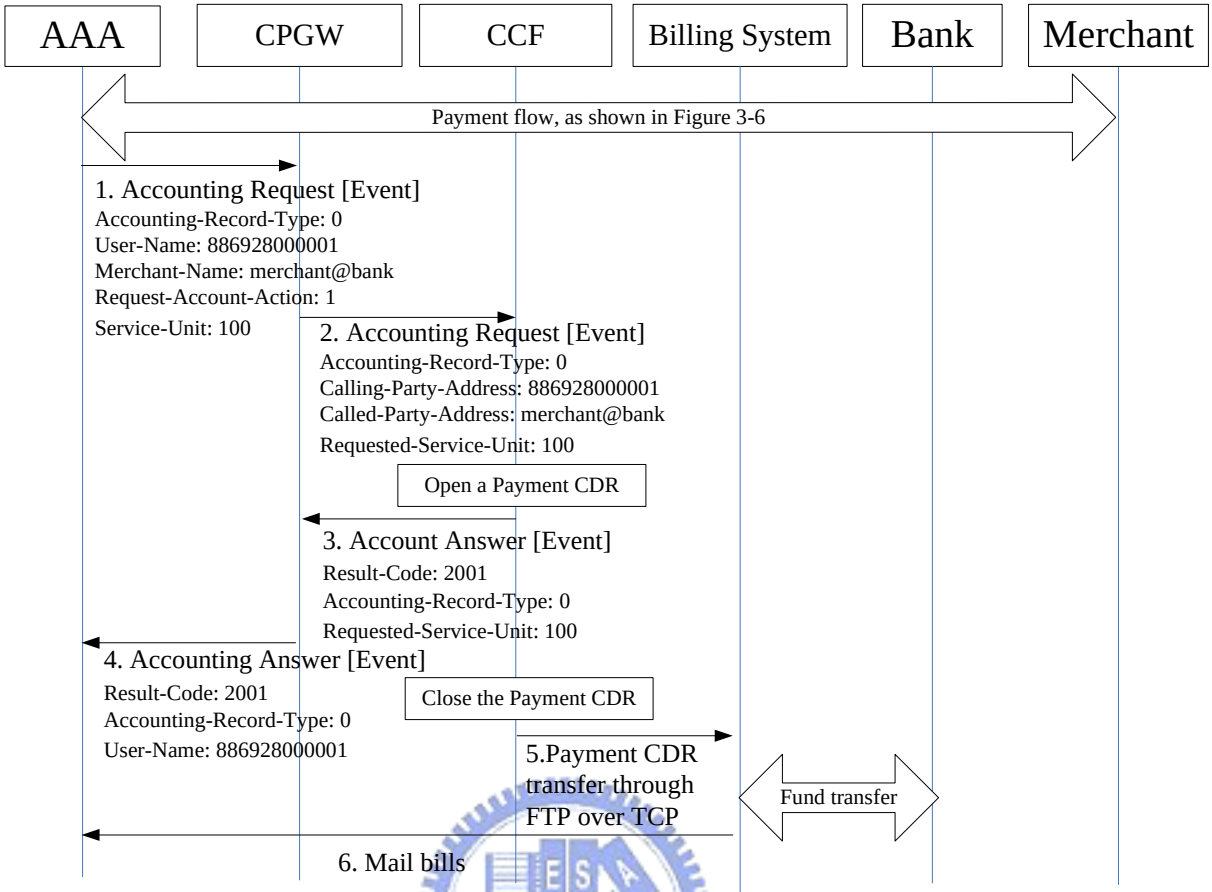

Figure 3-13: Payment flow for postpaid to third party account

Chapter 4 Implementation issues of the System

In this chapter, we describe the implementation issues of our prototype. First, we introduce our developing platform and programming tools. How the network entities of our architecture work together will be described later. We will also compare some mobile payment systems with our proposed solution.

4.1 The Platform and Tools

We have implemented our solutions including the SIP UA, AAA Server, and Merchant Server, the Payment-Gateway simulator on the Microsoft Windows Platform; HSS and WGSN on the Linux Platform. Except for HSS and WGSN, we use the Microsoft Visual C++ .Net Integrated Develop Environment (IDE) as our developing tool. The implementation requires socket programming and Diameter and SIP protocols using. We use SIP UA equipped with a SIM/USIM card as the Mobile Station. The following sections describe how each entity is implemented and work together.

4.2 The Network Entities

The SIP UA we used is the CCL SIP SkniUA was implemented by the Computer and Communication Research Laboratories (CCL) of the Industrial Technology Research Institute. We use SkinUA run in notebooks or PCs equipped with SIM/USIM card as the Mobile Station. The UA does not support the function of anonymous mobile payment; we enhance it with

accounting functions based on the Diameter protocol stack.

The main functions of the AAA server are authentication, authorization and accounting. The request/answer message between the AAA server and other entities in the network is based on diameter base protocol. First, when a MS equipped with a SIM/USIM card registers to AAA server for subscribing an anonymous mobile payment service, 3G authentication procedure will be arisen first. Second, AAA should authorize the user's privilege when user pays by using this service for shopping or content downloading. Figure 4-1 shows the flow chart of the registration and payment procedure.

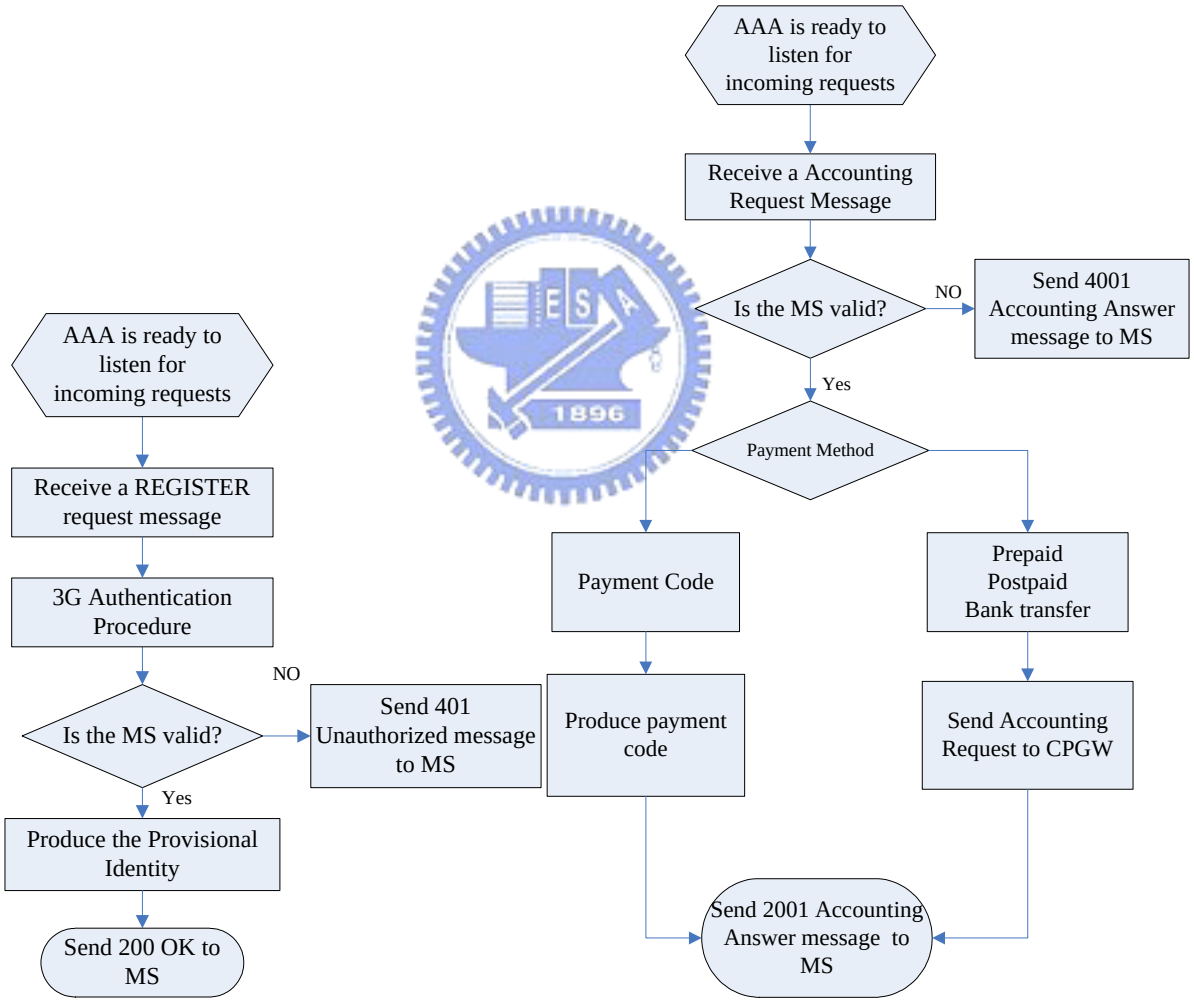

Figure 4-1: Flow chart of anonymous mobile payment service registration and payment

In order to utilize the existing 3G authentication mechanism, the AAA server cooperates with the HSS. The HSS produce authentication vectors to process a chain of verification. The HSS also store the user basic profiles for the 3G network service.

WLAN-based GPRS Support Node (WGSN) is a solution for integrating 3G and WLAN services. The 3G security mechanisms can be reused for WLAN user for the authentication and network access. A SIM/USIM card is used to store a user's profile and his or her private key. WGSN is used to attach the 3G network for the mobile device in our proposed solution. The mobile device is in the wireless access network.

The CPGW is responsible for the account transfer. The CPGW also can communicate with the third parties. The flow chart of the CPGW is shown in Figure 4-2. The Rf and Ro interface based on Diameter protocol are used to communicate with offline billing system and online charging system. The CPGW should use the two interface to transfer prepaid and postpaid accounts. And we use the Diameter protocol to transfer the transaction between the CPGW and the third parties.

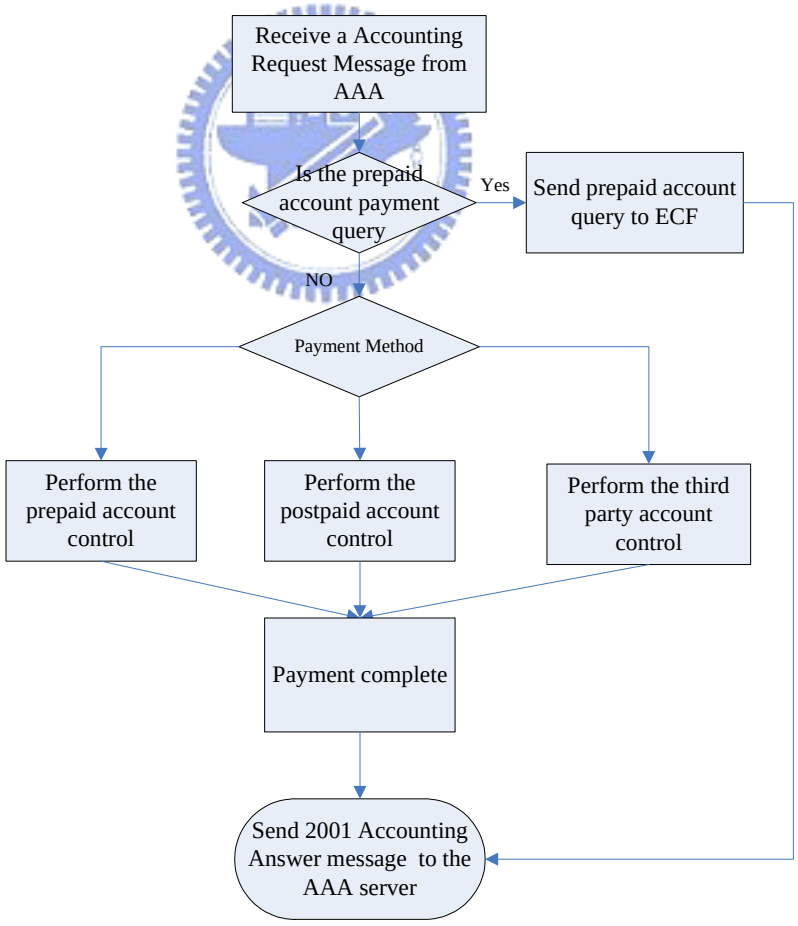

Figure 4-2: Flow chart of the Charging Payment Gateway payment

4.3 Comparison with other Mobile Payment System

4.3.1 Comparison with Sonera

Sonera MobilePay mobile payment solution has been introduced in section 2.4.1. We compare the payment procedure of MobilePay with our proposed solution. This payment scenario may be happened in these situations that a user and a merchant in the same mobile network or not. Moreover, a user and a merchant may belong to the members who register to the same third party. If a user wants to buy drink from a vending machine. He sends a payment request to AAA server with merchant identity by his mobile phone. AAA server assures that the vending machine has been registered by the merchant and sends notification to the vending machine. The vending machine will reply a result to AAA server. AAA server then sends the result to the user. The user gets the drink from a vending machine. At last, AAA server notifies the Charging Payment Gateway (CPGW) to make financial transfer. The CPGW depends on which payment account user chose in the first request message of the transaction to debit user's account and credit merchant's account. The procedure is shown in Figure 4-3. Our proposed solution provides more choices of payment methods such as prepaid, postpaid, bank account transfer, payment code request and cooperated third party account.

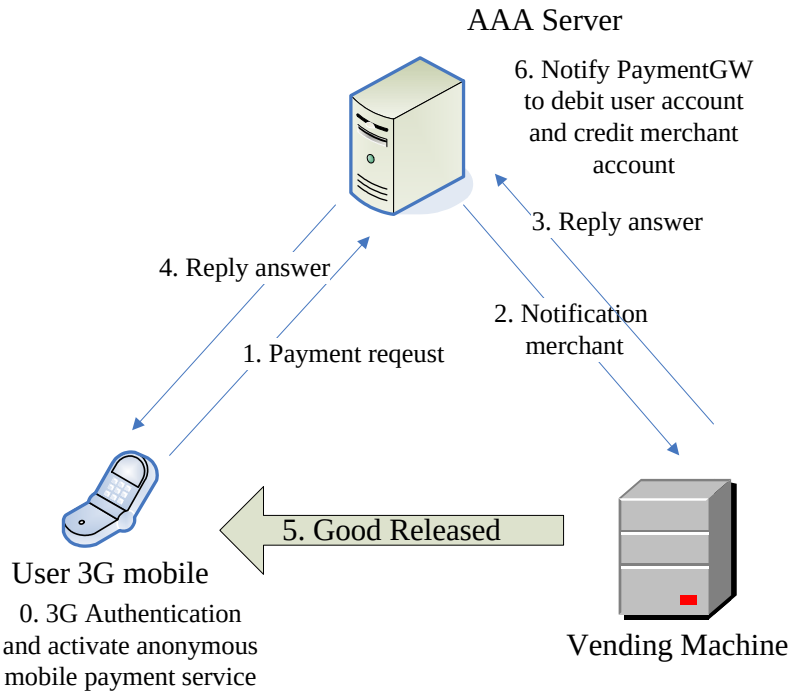

Figure 4-3: Our proposed anonymous mobile payment similar with Sonera MobilePay

4.3.2 Comparison with GiSMo

GiSMo mobile payment solution has been introduced in section 2.4.2. We can compare the payment procedure of GiSMo with our proposed solution. A user wants to buy goods from merchant web site and the merchant is not the user of mobile network as same as the user. The merchant may be in the internet or other networks. The user sends a payment code request to AAA server by his mobile phone. AAA server replies a payment code to the user. The user input the payment into his web form with his purchase to merchant's web server. The merchant's web server sends a request with the payment code to assure that the payment code is valid. The user gets the good from the merchant. At last, AAA server notifies the CPGW to make financial transfer. The CPGW depends on which payment account user chose in the first request message of the transaction to debit user's account and credit merchant's account.

The procedure is shown in Figure 4-4. We can provide more choices of payment methods

described in section 4.3.1, we also provide the mobility that GiSMo payment solution cannot support because GiSMo payment solution uses PCs with less mobility to purchase.

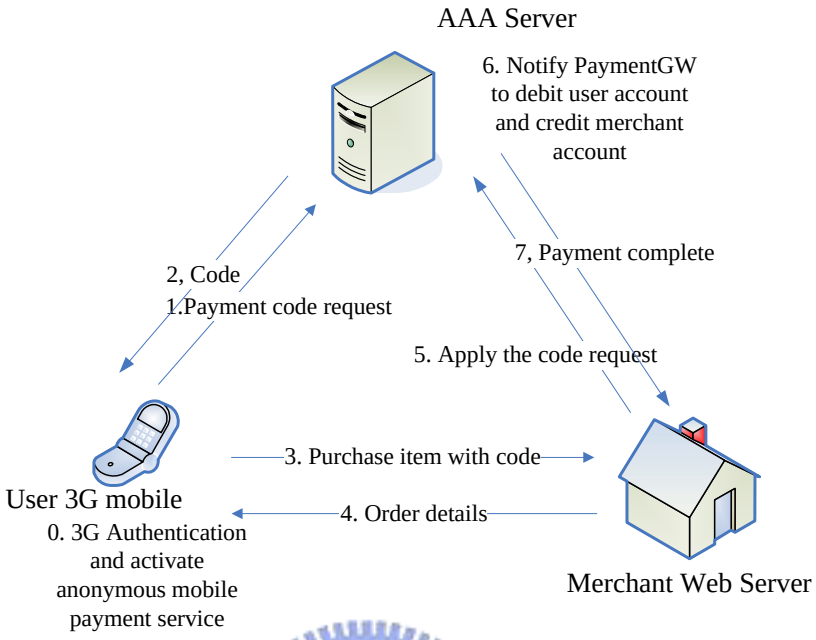

Figure 4-4: Our proposed anonymous mobile payment similar with GiSMo solution

4.3.3 The extension of the mobile payment with a third party

Banks or other financial service companies can take the third party role in a payment. A third party can provide account transfer to their customers through the network operator. Before, a network operator provides mobile access network service. Nowadays, a network operator can become a mobile payment service provider that can charges customers for their content service providers and make account transfer through the third parties. The network operator takes the financial service role; they also have their own content service providers.

Other mobile payment service providers, such as we have described in sections 2.4.1 and 2.4.2, are considered to be the third parties in our proposed solution and the third party cannot cooperate with a network operator. It means that if a user want to download the content from a content service provider who has signed a cooperation contract with the third party, they not

only should pass the authentication of the 3G networks but the authentication of the third party mobile payment service.

Though they are operator-independent, we can consider them as the extension of the mobile payment service a network operator provides. A network operator can provide the authentication procedure to the third party. A user can only pass authentication of the network operator one time and use the mobile payment services provided by third parties.

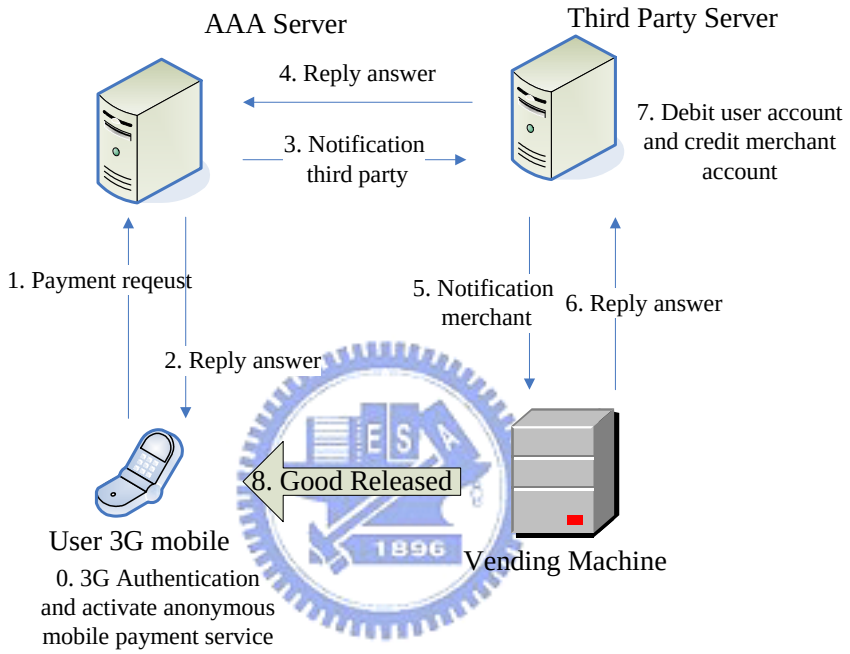

Figure 4-5: Our proposed anonymous mobile payment with third party

4.3.4 The Comparison of Mobile Payment Services

One significant advantage of a mobile payment system is that purchase can be charged directly to the subscriber's phone bill and administrated by a network operator in our proposed anonymous mobile payment solution. Sonera MobilePay and GiSMo mobile payment solutions are all operator-independent. They just use the resource of the mobile network as the data bearer. They need another third party account to support the payment system and are limited to some situations, such as less mobility in GiSMo payment system

and less extendable with other third parties in Sonera MobilePay payment system.

It is hard to compare the performance with these mobile payment services. Our proposed solution is for 3G networks and Sonera MobilePay, GiSMo mobile payment solutions are proposed in GSM networks. With the different conditions, we still can compare some features, such as Security, the variety of the payment method, independence, the anonymity and Mobility. The comparison is shown in Table 4-1.

Table 4-1: The comparison with other mobile payment solutions

	Security	Variety	Independent	User Privacy	Mobility
Our Payment Solution	Based SIM/USIM card authentication	Provide various payment methods	Network Operator as PSP and cooperate with third parties	Be hidden to the Merchant	Good
Sonera	Based on caller ID and PIN	Simple payment method	Independent PSP	User and merchant must register to Sonera	Good
GiSMO	Based caller ID and PIN	Simple payment method	Independent PSP	User and merchant must register to GiSMO	Bad
Paybox	Based caller ID and PIN	Normal payment method	Independent PSP	User and merchant must register to Paybox	Good
MobileSmart	Based on SMS and PIN	Simple payment method	Independent PSP	User and merchant must register to MobileSmart	Good

Chapter 5 Conclusion

Mobile payment is expected to grow rapidly in the near future. A lot of goods and services can be purchased using mobile devices and new business models will be developed. 3G mobile networks have defined charging principles specifying how the users are charged by the resource or services they use. To provide a mobile payment service, it is suitable to be fully integrated with the 3G Networks.

We have investigated mobile payment infrastructure for B3G (Beyond 3G) network. We design a mobile payment system that enables a subscriber to make payment to a VASP (or merchant) through the network operator and remain anonymous to the VASP. The customer can be a prepaid subscriber or postpaid (monthly bill) one. 3G authentication can be reused. In addition, we have developed a charging and payment gateway, and an AAA server to perform the following functions: 1). Interwork the mobile payment with the existing prepaid and postpaid billing system of the UMTS network. 2). Interwork with existing electronic payment systems to make payments to VASPs

Chapter 6 Reference

[1] DONAL O'MAHONY, Electronic Payment Systems for E-Commerce 2nd Ed, Artech House, 2001, Boston andLondon

[2] M. Peirce, "Multi-Party Electronic Payments for Mobile Communications" Ph.D. Thesis, University of Dublin, Trinity College, Oct. 2000.

[3] William Stallings, Network Security Essentials: Applications and Standard, Prentice Hall, Nov. 1999

[4] David Chou, Yu-Sheng Lin, E-commerce Industry Yearbook 2003, Market Intelligence Center(MIC), Institute for Information Industry, July 2003, ROC.

[5] 3GPP TS 32.200 "Charging management; Charging principles (Release 5)", June 2003.

[6] 3GPP TS 32.205 "Charging management; Charging data description for the Circuit Switched (CS) domain (Release 5)", June 2003.

[7] 3GPP TS 32.215 "Charging management; Charging data description for the Packet Switched (PS) domain (Release 5)", June 2003.

[8] 3GPP TS 32.225 "Charging management; IP Multimedia Subsystem (IMS) (Release 5)", June 2003.

[9] 3GPP TS 32.235 "Charging management; Charging data description for application services (Release 5)", June 2003.

[10] 3GPP TS 33.102 "3G Security; Security architecture (Release 6)", September 2003.

[11] 3GPP TS 24.228 "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3 (Release 5)", June 2003.

[12] P. Calhoun Airespace, Inc., "Diameter Base Protocol" RFC 3588, IETF, September 2003.

[13] 3GPP TS 29.228 "IP Multimedia (IM) Subsystem Cx and Dx Interface; signalling flows and message contents (Release 5)", June 2002.

[14] J. Rosenberg, Henning Schulzrinne, G. Camarillo, E. Schooler, Mark Handley et al., “SIP : Session Initiation Protocol”, RFC 3261, IETF, June 2002.

[15] Toshiba America Research, Inc., “opendiameter-src-1.0.0,” OpenDiameter: open-source software for the Diameter protocol, 2002