Online Payment for Access to Heterogeneous Mobile Networks

Version: 14 Feb 2002

Heiko Knospe[1], Scarlet Schwiderski-Grosche[2]

[1]T-Systems Nova GmbH,
Technologiezentrum ES21d
D-64307 Darmstadt,
Tel: +49 6151 832033, email: heiko.knospe@t-systems.com
[2]Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
Tel. +44 1784 414346, email: Scarlet.Schwiderski-Grosche@rhul.ac.uk

ABSTRACT

This paper describes an architecture where access to heterogeneous mobile networks is granted on the basis of online payment methods. Access methods for GSM networks were designed for subscribed post-pay customers. With the Intelligent Networks (IN) technology, the operators could also offer services to prepay customers. Now online payment might provide additional means for network access. We suggest an IP based architecture which uses a Diameter application (successor of Radius) for cost control and a charging component for online payment.

I. Introduction

A. Access for subscribed post-pay customers

In the past, access to mobile networks was reserved for subscribed customers. There, when someone signs up with a GSM network, the operator usually checks the credit status of its potential customer to protect against financial loss. The customer is handed out a SIM card with a shared secret key *Ki*, which enables him to authenticate towards the GSM network. He is then authorised to use the subscribed services. The records on his service consumption are collected and after some time (e.g. within a day) transferred to a rating and billing system for post-processing. The call detail records are rated (i.e. a price is assigned to them) and then aggregated to a (monthly) bill. This will probably remain the standard access scenario for future UMTS networks, and post-pay customers remain the main target group for mobile operator.

B. Growing prepay market

Although the post-pay scenario offers advantages in the operational and marketing model of the operator, there is a growing demand for prepaid GSM services. These offer protection against losses for the network operator and cost control for the customer. Prepay access services open up a new market. Prepay customers are also given a SIM by which they authenticate to the network. Before being able to use services (e.g. set up a call) the prepay account has to be charged. From a network point of view, prepay services are realised using IN (Intelligent Network) components. At call setup and also during the call, the IN controls the connection and interrupts it if resource consumption surpasses the charged amount (cf. section II for more details). Because of technical and marketing reasons, network operators may not offer all services (e.g. roaming, GPRS) to their prepay customers.

C. Online payment

The SHAMAN (Security for Heterogeneous Access in Mobile Applications and Networks) project addresses the protection and security required for users, information and services in future mobile telecommunications systems [9]. One future requirement is to provide flexible means for accessing heterogeneous mobile networks, which not only involves GSM, GPRS, and UMTS, but also WLAN, Bluetooth, or other network technologies. In this paper, we address work being done in SHAMAN, namely investigating the option to grant network access based on online payment. Existing payment protocols should be used (cf. section III). A mechanism for real time accounting and related service control will be required. Since IN services are not available in all cases (e.g. WLAN), we suggest to use IP-based protocols (cf. section IV).

II. Service Control in GSM, GPRS, and UMTS networks

A. IN-based prepaid services for GSM

Soon after the introduction of GSM networks, the idea arose to introduce standardised IN services. The GSM extension was called CAMEL (Customised Application for Mobile Enhanced network Logic). CAMEL adapted parts of the fixed net standard ETSI Core INAP.

Designed for circuit switched calls (CAMEL phase 1 and 2, cf. [4]), the idea is to trigger the IN during call handling at the MSC (Mobile Switching Center) if the HLR (Home Location Register – the location where

subscriber parameters are stored) entry indicates subscription of an IN service.

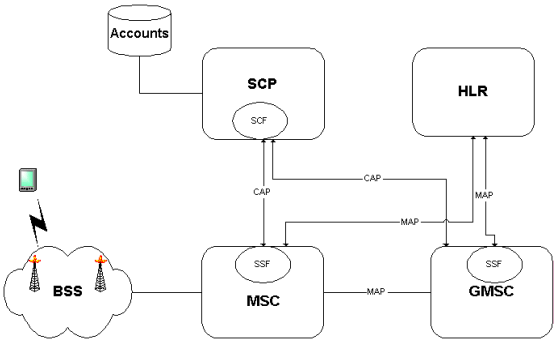

Figure 2: IN involvement for GSM calls

All protocols are based on the Signaling System number Seven (SS7). The SCP (Service Control Point) controls the call via the Camel Application Part (CAP) protocol. With the support of the IN, a number of services can be realised. A prominent feature is the transformation of dialled numbers (e.g. to realise Virtual Private Nets).
Another IN application are prepaid services. Then a customer database keeps track of the credits. There are several possibilities to replenish, e.g. the customer can activate a previously bought token. For calls from prepay customers, the IN is always triggered. The SCP checks the user's account before allowing the call setup to be completed. The SCP (pre-)rates the call and informs the MSC about the maximum call period. During the call, the SCP keeps a connection with the MSC which informs the SCP about the call status. The SCP performs hot-rating, decrements the user's account, and interrupts the call if necessary. Although roaming scenarios are not discussed here, it should be noted that in any case the SCP (and HLR) of the home network is involved.

B. Prepaid services for packet switched networks
With CAMEL phase 3 (which is part of UMTS release 99), IN services for packed switched networks (GPRS, UMTS) were introduced (cf. [5]). Here the SGSN (Serving GPRS Support Node) plays a similar role as the MSC in circuit switched networks. The mobile station requests a PDP (data) context from the SGSN. The SGSN first authenticates the user. Then the SGSN requests creation of a PDP context from the GGSN (Gateway GPRS Support Node).
If the operator has implemented prepaid GPRS services with CAMEL phase 3, then the IN is involved during the data context creation. The SGSN triggers the SCP, which checks the user's account as in the circuit switched case. The SGSN updates the SCP in regular intervals with status information (time, volume, position) about the PDP context. The SCP performs hot-rating, decrements the account, and requests the SGSN to continue processing or to release the PDP context.
Depending on the number, the duration and the traffic of the GPRS sessions, this can impose important performance requirements on the SGSN, SCP and their involved functional entities (gprsSSF and SCF).

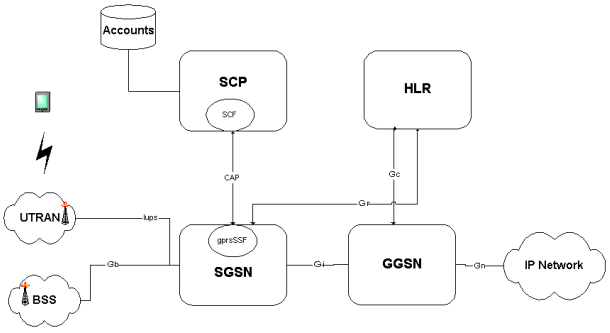

Figure 1: Prepaid services with CAMEL phase 3

We remark that also for IP services, authentication relies on GSM or UMTS SIM card-based security functions. Accounting data on service usage is collected at the SGSN. Currently, IP based components, such as AAA server, play a secondary role.

III. Background on electronic payment systems

Electronic payment systems provide means for payment of goods or services over the Internet. In contrast to conventional payment systems, the customer sends all payment-related data to the merchant over the Internet; no further external interaction between customer and merchant is required (e.g. sending an invoice by mail or confirmation by fax). To date, there exist more than 100 different electronic payment systems [1].
With the emergence of mobile commerce applications, more and more electronic payment systems are being developed for employment in a mobile context. These *mobile payment systems* use a mobile device (e.g. a mobile phone or a PDA) for exchanging payment-related data via a public mobile network with the merchant [3].
In our scenario, the customer is presented by the user associated with a MN and the merchant is presented by the access network operator.

A. Distinctive features of payment systems
The following list gives an overview of some distinctive features of electronic payment systems:
1. *time of payment*
2. *payment amount*
3. *anonymity issues*
4. *security requirements*
5. *online or offline validation*

1. *Time of payment* denotes the relation of the initiation of a payment transaction and the actual payment. In *pre-paid payment systems*, the customer's account is debited before the payment and the amount is stored, for example, on smart cards, in specific customer accounts or as electronic cash. In *pay-now payment systems*, the customer's account is debited at the time of payment (for example, ATM card or debit card with PIN) and in *post-payment systems,* payment can be regarded as a "payment promise" where the merchant's account is credited before the customer's account is debited (for example, credit card systems).
2. The *payment amount* has an influence on the design of electronic payment protocols. For example, payments in the order of 1€ are only viable, if the incurring

computational and communications overhead is kept small. Accordingly, there is a distinction between

- *micropayments* (up to about 1 €)
- *small payments* (about 1 to 10 €)
- *macropayments* (more than about 10 €)

3. Electronic payment systems often originate with conventional payment systems. As such, cash-like payment systems should provide *anonymity* to the customer. There are different degrees of anonymity: complete anonymity means that the customer remains anonymous to the merchant and the bank. However, in many payment systems, only partial (or no) anonymity can be provided.

4. The *security requirements* of electronic payment systems differ. Generally, integrity, authentication, authorisation, confidentiality, availability, and reliability issues need to be considered, depending on the specific requirements of an electronic payment system.

5. *Offline payment validation* means that no third party (e.g. a bank or credit card institution) is involved during the payment procedure, whereas *online payment validation* involves some kind of authorisation server. The latter causes an additional communication overhead, but reduces certain risks, e.g. double spending.

The above discussion summarises some distinctive features of electronic payment systems. There are other issues such as

- overhead for customer and merchant (in terms of installation of software, registration, etc.)
- performance
- charge per payment transaction
- ACID principle for payment transactions
- national or international employment

The list of distinctive features gives an idea of the complexity and variety of electronic payment systems.

B. Examples of electronic and mobile payment systems

Electronic payment systems are typically modeled on conventional payment systems. As such, there are the following categories:

- Electronic cash – the customer withdraws money from his bank, hands the payment tokens to the merchant, who deposits them with his bank.
    - Examples: eCash and GeldKarte
- Credit card-based – the customer hands his credit card data to the merchant, who submits it to his bank for online validation. Actual payment is done via the established financial network.
    - Examples: SET and CyberCash
- Cheque-like – the customer hands a payment authorisation (cheque) to the merchant, who presents it to his bank, which redeems it from the customer's bank.
    - Examples: BankNet and NetCheque
- Bank transfer – the customer instructs his bank to transfer funds to the merchant's account.
    - Examples: AIMP and NetFare

For a description of these and other payment protocols, see [1, 2]. [2] gives a good overview of the background of payment systems.

Most electronic payment systems are not suitable for employment in a mobile context, i.e. using a mobile device and/or communicating over a public mobile network. This is due to limitations of memory, processing power and bandwidth. Moreover, the limited size of the display makes an adaption of the software necessary. On the other hand, mobile devices offer advantages such as ubiquity, accessibility and security. For example, whereas some electronic payment systems require secure hardware such as smart cards and smart card readers, this is inherent in mobile devices (SIM cards). Some examples of mobile payment systems are [3]:

- Dual-slot mobile phone (Paiement CB sur mobile)
- Dual-SIM mobile phone (EMPS – Electronic Mobile Payment System)

Issues for applying electronic and mobile payment systems for access to heterogeneous mobile networks will be discussed in section IV.

IV. Access based on alternative means

A. Network Architecture

The current situation of mobile networks in Europe indicates a growing diversity in future network access technologies. Apart from GSM, GPRS, and UMTS, there will probably coexist WLAN (IEEE 802.11b, 802.11a), Hiperlan/2, Bluetooth, and maybe others.

We follow the approach of the BRAIN project (cf. [6]). The core network (called BRAIN access network) is an all-IP operator network with access routers (AR) at the edge, gateways towards the public Internet, and an AAA infrastructure. The mobile node uses one of the existing radio technologies to set up an IP link to the access router. The approach is to use standard access procedures, which are independent of the radio technology. AAA procedures are initiated by the AR, which acts as AAA client in the BRAIN access network. The AAA server is usually located in the home network of the subscribed customer.

B. Access Procedures

The access procedures will differ according to the kind of commercial relationship between the customer and the operator. Subscribed customers can be authenticated by their home operator, so that AAA requests are relayed to their AAA home server. Here, we focus on customers who wish to use a network, which they have not subscribed, neither directly nor indirectly as a roamer. Assuming that the operator does not grant free access, the mobile user will then be requested to pay for the access. The various possibilities of electronic payment were discussed in section III above. The challenge is then to combine AAA with online payment procedures.

In this setting, there are reasons to suggest an approach which differs from current IN-related prepay scenarios (cf. section II):

- The IN prepay service does not offer integrated online payment, although this might change with future developments.
- The IN prepay services were designed for circuit switched networks and then extended to GPRS/UMTS networks but do not apply to all-IP networks.
- The IN approach is not compatible with Internet accounting principles.

The approach presented here resolves these problems. But we also discuss below some disadvantages of this approach.

C. Real Time Accounting

The proposed architecture relies on the following components:

- The AR acts as AAA client
- There is no AAA home server, access is handled by the local AAA server
- The AAA server delegates real-time accounting and service control to a component called "Credit Control Server" (CCS) which uses a Diameter application towards the AR (cf. [7], [8])
- The CCS delegates payment-related tasks to a new component called "Cost Charging Center" (CCC)
- The CCC communicates with the Background Payment systems

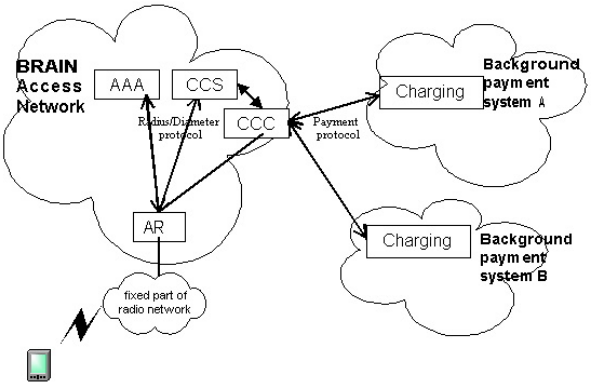

Figure 3: Architecture for payment controlled access

In the following, we give a brief overview over the major protocol steps:

1. The mobile station attaches to the radio network and obtains an IP address from the access network (e.g. by IPv6 stateless autoconfiguration). IP traffic is still barred at the AR as long as AAA procedures have not been finished successfully.
2. Setup of encryption and integrity protection between the MN and the AR. Since MN and AR may have no prior security relationship, public key cryptography shall be used to establish a common secret key. The AR may authenticate towards the MN with a certificate.
3. The AR as the AAA client sends the client's access request to the local AAA server using the Radius or the Diameter protocol. The client might have a temporary identity or even be anonymous. In order to avoid additional protocol exchange with the CCC later on (step 7), the client might send payment related data as its user identity.
4. The AR gets the information from the AAA server to forward accounting data to the CCS. Access must not yet be granted before the first accounting interrogation is successful.
5. The BAR sends a first accounting record (Start Record) via the Diameter protocol to the CCS and requests a number of service units (time, volume), cf. [x].
6. The CCS rates the requested units and delegates to the CCC in order to recharge the account.
7. The CCC performs the payment protocol with a background payment system (see details below).
8. The CCC sends information about the confirmed amount to the CCS.
9. The CCS sends an accounting answer via the Diameter protocol to the BAR. The answer contains the number of granted service units (time, volume).
10. The AR grants network access to the MN.
11. The AR (diameter client) updates the CCS via the Diameter protocol regularly with information on service usage (Interim Records). The AR may also request new service units from the CCS. The CCS performs online rating and updates the CCC.
12. Upon user request, timeout or when granted service units are exhausted, the AR interrupts the connection with the MN and sends a Stop Record message via the Diameter protocol to the CCS. The CCS closes the accounting record and informs the CCC about the total amount due.
13. The CCC performs the final billing. Depending on the payment protocol, the customer may now be eventually charged or refunded.

In the following, we mention restrictions and disadvantages of this approach:

- Mobility Management and roaming scenarios respectively are not integrated.
- The customer is charged whenever traffic passes the AR, although the packets may not finally arrive over the radio link at the MN.
- Interim Accounting Records between AR and CCS may produce heavy traffic and load on these components.

D. Online payment

In steps 6 to 8 of the real-time accounting protocol (see section IV.*C*), the control flow is passed to the CCC in order to perform the payment protocol with a background payment system. After performing the payment protocol, the CCC sends information about the confirmed amount back to the CCS.

Practically, the CCC implements the merchant's payment functionality, that is, the merchant payment software specific to a payment system is installed on the CCC. When the work is delegated from the CCS to the CCC, the specific payment software is triggered. The corresponding background payment system validates payment transactions either online (during the payment) or offline (at some later point in time).
Since an access network operator may support multiple payment protocols, the merchant payment software for each one of them needs to be installed on the CCC.
The goal of this section is

1. to identify the requirements imposed on the payment protocol
2. to determine the parameters required from the CCS for performing the payment protocol
3. to propose classes of payment protocols suitable for real-time accounting

1) The scenario described in this paper differs from the traditional electronic payment scenario in that the transaction amount can only be established at the end of the connection. However, a *payment guarantee*, possibly stating a maximal transaction amount, has to be given at the beginning of connection establishment in order to assure the CCS in the access network.
In traditional payment scenarios, the customer (here, the user of a MN) can be contacted when the total transaction amount is available. Payment is then performed between the customer and the merchant (here, the access network operator). In our scenario, determining the total transaction amount means that the user has interrupted the connection and hence, cannot be contacted anymore.
The charge for single service units will typically be in the order of micropayments. Hence, a micropayment protocol seems suitable. However, depending on the specific connection, the total amount can add up to small or even large payments. For this reason, payment protocols for small and macropayments should not be ruled out.
In our scenario, the user uses a mobile device for exchanging payment-related data via a public mobile network with the access network operator. For this reason, the chosen payment protocols need to deal with the inherent limitations.
Since the payment protocol is performed in real-time, there must be an upper limit to the timely overhead it imposes. Therefore, a payment protocol requiring multiple communications between MN and background payment systems may not be suitable.
Depending on the payment protocol, specific security mechanisms are in place on the application level (often based on public-key techniques). Additionally, the access network specific security mechanisms are implemented.

2) When the control flow is passed from the CCS to the CCC (in step 6 of the real-time accounting protocol), the CCC will need certain parameters in order to run the specific payment protocol. These parameters are (or include)

- selected payment protocol
- BAR identifier
- identifier of the MN or (temporary or permanent) identifier of the user
- estimated cost of service event
- depending on the payment protocol, payload with information regarding the specific payment protocol (e.g. credit card information or authentication information of the user for the payment protocol).

3) There are two possibilities for payment:

1. There is a *user-specific account in the background payment system*, from which open bills can be settled. The user will have initially authorised payment up to a certain amount and the bill can be settled without further user interaction.
2. *Tokens* with a monetary value (e.g. electronic cash) *are stored on the MN* and money is debited from the MN in regular intervals, when the CCS requests a number of service units. Since tokens cannot be credited to the MN once the user has disconnected, the requested number of service units needs to be reasonably small in order to make monetary loss negligible.

The main advantage of the first possibility is that the user does not have to be contacted after initial authentication and authorisation, as long as the maximal transaction amount is not exceeded. Hence, this solution will reduce the communication overhead between MN and CCC. On the other hand, the second possibility has the major advantage that, in principle, the user can remain completely anonymous. Instead of an authentication message, the user sends payment tokens that allow access regarding a number of service units. The background payment system needs only to be involved for verifying the validity of the payment tokens.
In the course of the SHAMAN project, we will investigate several payment protocols regarding their suitability. These are credit-card and account based payments in the first category and eCash and GeldKarte in the second.

V. Conclusions

The paper presents an approach how to combine access and service control for mobile networks with payment protocols. The Diameter base protocol and its applications may be used for cost control and an extension to online payment procedures seems feasible. Additional work has to be done to define the protocol details and to analyze the suitable electronic payment systems.

REFERENCES

[1] ePayment Systems Observatory, database on e-payment systems, http://epso.jrc.es/

[2] R. Weber, " Chablis - Market Analysis of Digital Payment Systems", Technical Report TUM-I9819, TU Munich, 1998, http://chablis.informatik.tu-muenchen.de/Mstudy

[3] T. Weitzel, "Vom E- zum M-Payment", http://much-magic.wiwi.uni-frankfurt.de/profs/mobile/infos.htm.

[4] 3GPP TS 03.78 version 7.7.0 Release 1998
[5] 3GPP TS 22.078 version 4.4.0 Release 4
[6] IST-1999-10050 BRAIN D2.1, BRAIN Access network requirements, specifications and evaluation of current architectures and technologies and their requirements: core network and air interface
[7] P. Calhoun, H. Akhtar, J. Arkko, E. Guttmann, A. Rubens, G. Zorn, „Diameter Base Protocol“, draft-ietf-aaa-diameter-08.txt, IETF work in progress
[8] H. Hakala, S. Karlsson, „Diameter Credit Control Application“, draft-hakala-diameter-credit-control-01.txt, IETF work in progress
[9] IST-2000-25350 SHAMAN, http://www.ist-shaman.org/ .