Trialling Secure Billing with Trusted Third Party Support for UMTS Applications

G. Horn[1], P. Howard[2], K. M. Martin[3], C. J. Mitchell[4], B. Preneel[3] and K. Rantos[4]

1. Siemens AG, Corporate Technology, D-81730-München, Germany
2. Vodafone Ltd., CSAD, 2-4 London Road, Newbury, RG14 1JX
3. Katholieke Universiteit Leuven, ESAT-COSIC, B-3001 Heverlee, Belgium
4. Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 0EX, U.K.

Abstract: *We present a protocol developed by the ASPeCT project for secure billing that provides the incontestable charging that is required for UMTS. This protocol realises a payment system for value added services. We describe the protocol and in particular the design features that are of particular relevance to the UMTS environment. We also describe the configuration of a field trial of this protocol over the experimental UMTS platform developed by the project EXODUS.*

1 Introduction

In this paper we present a protocol for secure billing that can provide the incontestable charging required for the third generation mobile communications system, also known in Europe as UMTS (*Universal Mobile Telecommunications System*). This protocol has been developed by the project ASPeCT (*Advanced Security for Personal Communications Technologies*) and following successful demonstration in 1997, the protocol will be tested in May 1998 in a field trial over the experimental UMTS platform developed by the project EXODUS (*Experiments on the Deployment of UMTS*). The protocol has been integrated at the application level (realising a payment system for value-added services) rather than into the basic UMTS security services, but it has been designed in a way that permits this development in the future. The demonstrator and the trial also take into account the requirements of *Trusted Third Parties* (TTPs), and in particular the need for cross-certification scenarios. In the following discussion we motivate both the goals of the protocol and the particular design principles that make the protocol a particularly suitable candidate for providing electronic commerce support in UMTS. We follow this with a short description of the protocol and then describe the configuration of the field trial.

2 Motivation and Protocol Design

2.1 Mobile Information Services

A significant difference between existing second generation telecommunications systems such as GSM and future third generation systems such as UMTS will be the variety and number of *value-added services*, such as on-line information services, that a user will be able to purchase over the network. These services will be provided by an ever-increasing number of competing *value-added service providers* (VASPs) who will in turn be serviced by a large number of different public and private network operators. Within this complex mosaic of network relationships it is clear that there exists a great need for incontestable charging procedures to permit payments for value-added services to be made reliably and with minimal risk of fraud

2.2 Protocol Goals

The basic ASPeCT protocol for secure billing within UMTS operates between a mobile user and a VASP. The ultimate goal of the protocol is to establish billing information that acts as incontestable evidence that the user has committed to pay a certain amount for a valued-added service. We assume

that the actual payment claim, and ultimate billing of the user, takes place off-line with the assistance of the user's UMTS service provider and these processes are not a feature of the ASPeCT demonstrators or trials. The protocol is in fact divided into two separate component protocols whose goals we now describe.

2.2.1 Authentication and Initialisation Protocol

The two general aims of this protocol are to establish various degrees of authentication between the user and the VASP and to initialise the subsequent payment protocol. More precisely some of the main goals are:

- mutual explicit entity authentication (assurance that each entity is who they claim to be);
- mutual agreement on a secret session key;
- mutual implicit key authentication, key confirmation and key freshness (assurance that only the other entity could possibly also know the agreed session key, assurance that the other entity actually has possession of the agreed key, and assurance that it is a new key);
- non-repudiation by the user of initialisation information sent to the VASP;
- confidentiality of the user's identity (at the interface between the user and the VASP).

2.2.2 Payment Protocol

The payment protocol describes a mechanism for making payments for a value-added service. The goal is to establish an incontestable bill for the total amount due to the VASP (payee) by the user (payer). More precisely some of the goals are:

- the user is assured that the amount of the payment will be precisely that specified on the bill and that only the intended VASP can receive the payment;
- the VASP is assured that the user cannot deny having incurred the bill and can be certain of receiving the exact amount of the payment specified on the bill.
- an external broker (probably the user's UMTS service provider) can verify the correctness of the bill in order to assist in the clearing of the payment.

2.3 Protocol Design Issues

The design of the ASPeCT protocol was directly targeted towards the UMTS environment. This reflects itself in a number of important ways, which we now detail.

2.3.1 Protocol Scenario

The adopted protocol scenario is well suited to the mobile environment as the roles required can be played by entities already active in current mobile networks, namely mobile users, mobile services providers and VASPs. Their existing business relationships, in particular the existing infrastructure for billing users for telecommunications services, can thus also be adopted for payment of value-added services without the need for additional clearing network or financial institutions such as bank or credit card organisations.

2.3.2 Authentication Mechanism

The authentication protocol between user and VASP is based on a protocol submitted to ETSI (*European Telecommunications Standards Institute*) for user-to-network authentication [3]. The significance of this is that the ASPeCT protocol can also be used for user-to-network authentication and hence payment for value-added services and basic telecommunications services can be efficiently combined by integrating the initialisation of payment process with call set-up procedures in UMTS.

2.3.3 Payment Mechanism

The fundamental design factor behind the payment mechanism is the recognition that the unit cost of value-added services will be very low and hence communication and processing costs of charging for such services must be kept to a minimum. Payment mechanisms for this type of transaction are often

known as *micropayment schemes* and have already been proposed for diverse applications such as electronic publishing and video-on-demand. The micropayment technique adopted by ASPeCT is based on the *tick payment protocol* of [10], (see also [1,4,8,11,12]). This mechanism was selected because it is extremely lightweight and its initialisation could be incorporated naturally into the proposed authentication process.

2.3.4 Cryptographic Technology

A significant difference between the cryptographic techniques used within ASPeCT and those used in current telecommunications systems is the adoption of *public key* cryptographic techniques. While these traditionally involve greater computational overheads, improvements in smart card technology allow the exploitation of the increased flexibility and range of services that such technology can provide. The cryptographic technology used in the ASPeCT protocol was primarily selected in order to suit the low bandwidth and low computational capabilities on the user's smart card. Some precise reflections of this requirement include:

- use of digital signatures with small storage overhead (International Standard ISO/IEC 9796-2 [6] and the elliptic curve signature scheme under consideration in ISO/IEC 14888-3 [7]);
- a message exchange system that concentrates all costly non pre-computable exponentiations at the VASP end of the communication if the preferred elliptic curve signatures are used;
- use of elliptic curve cryptosystems to reduce the length of messages.

2.3.5 Public Key Infrastructure

Applying public key techniques in a complex network necessitates the existence of a *public key infrastructure* (PKI). This includes TTPs who act as *certification authorities* (CAs) for entities such as mobile users and VASPs (specifically, a TTP will produce a *certificate* which provides a guaranteed link between the identity of an entity and a public key). The full version of the ASPeCT authentication and initialisation protocol includes a message exchange between the VASP and the TTP of the user in order to ensure that both the user and the VASP are able to verify the certificates of one another's public keys. Since the user and VASP may well be in different domains this involves the creation of *certificate chains.* The specific TTP services and protocols used by ASPeCT are also targeted towards UMTS. In particular, the certificate format has been chosen in order to minimise the storage space on the smart card and the bandwidth of the air interface (a public-key certificate is less than 200 bytes, which compares favourably with the 1Kbyte needed for a typical X.509 certificate).

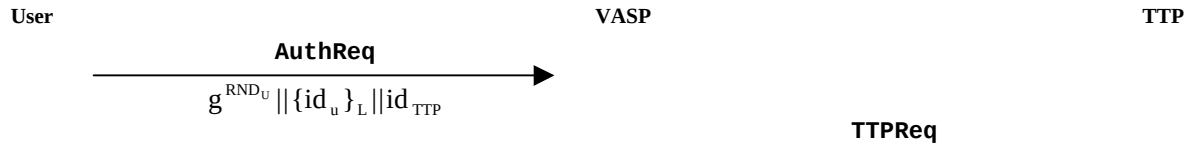
3 Protocol Description

We provide a very brief description of the ASPeCT protocols here. For full details and explanations of the working of the protocol see [5,9].

3.1 Prerequisites

All entities have access to a strong symmetric encryption function, where $\{M\}_K$ denotes the encryption of M using key K. Functions $h1$,$h2$ and $h3$ are all implemented using the one-way hash function RIPEMD-128 [2], but for their precise theoretical requirements see [5]. The VASP has a long term secret/public key agreement pair (v,g^v), where g is the generator of a finite group in which the *Discrete Logarithm Problem* is hard.

3.2 Authentication and Initialisation Protocol



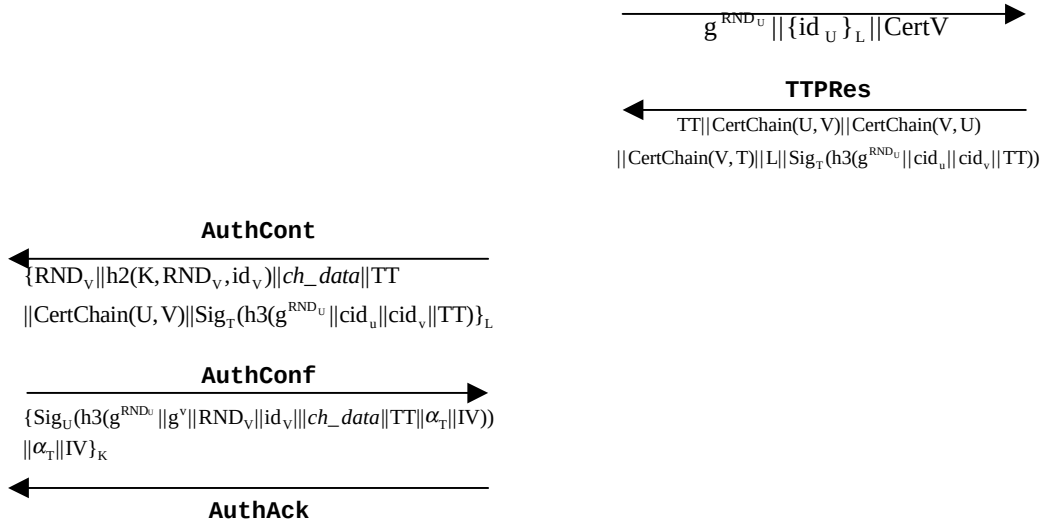


Figure 1: Authentication and Initialisation Protocol

The main steps of the authentication and initialisation protocol shown in Figure 1 are as follows. The user generates a random number RND_U and sends a request **AuthReq** to the VASP, including the identity of the user's TTP and the user's identity, encrypted by a key L computable by the TTP. The VASP forwards most of this message along with its public key certificate in **TTPReq**. The TTP replies to the VASP in **TTPRes** with several certificate chains (where *CertChain*(*X*,*Y*) allows entity *X* to verify the certified public key of entity *Y*), a timestamp *TT*, key *L* and a signature on data that includes two certificate identifiers. The VASP generates a random number RND_V and sends **AuthCont** to the user, which includes the tariff information *ch_data* and the information necessary for the user to compute the shared key $K=h1((g^{RNDu})^v || RND_v)$, all encrypted using key *L*. In **AuthConf** the user replies by sending the VASP an encrypted signature on information that includes parameters *IV* and α_T which are needed to initialise the payment protocol. The VASP acknowledges receipt in **AuthAck**. This protocol achieves all the goals specified in Section 2.2.1 (for details, see [5]).

3.3 Payment Protocol

The payment protocol assumes that during initialisation the VASP has received the values *IV* (a random value selected by the user that identifies a one-way function F_{IV} from a family of such one-way functions), and the value $\alpha_T = F_{IV}^{\ T}(\alpha_0)$ which is generated from a random value α_0 generated by the user. The user pays for units of service by releasing pre-images of α_T. The basic payment protocol exchange is shown in Figure 2.

On receiving a demand for the first *d* units of payment (*ticks*) from the VASP, the user makes the payment commitment by releasing the appropriate pre-image value $\alpha = F_{IV}^{\ T-d}(\alpha_0)$, which the VASP can easily verify by checking that $\alpha^d = \alpha_T$. To pay for the next *d*2 ticks the user will then commit with the value $\alpha = F_{IV}^{\ T-d-d2}(\alpha_0)$, and so on. Once *T* ticks have been purchased then a re-initialisation process must be run.

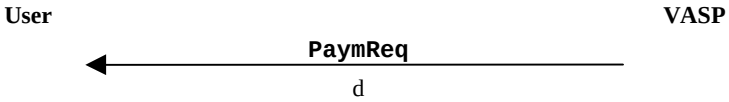


Figure 2: Payment Protocol

When the call session has ended the VASP stores the last received pre-image α and the number of ticks consumed by the user during the current protocol run and composes and stores the transcript of the charge ticks transaction, representing the bill to be later claimed. The information contained in the transcript includes the signature received from the user in **AuthConf** of the initialisation protocol. Again, for further details that the Payment Protocol achieves the goals of Section 2.2.2, see [5].

4 Trial Configuration

The configuration of the ASPeCT Secure Billing Trial is shown in Figure 3. The trial will run over the EXODUS experimental UMTS platform. The three entities, mobile user, VASP and TTP, will be implemented on three different devices, with fixed broadband access to the EXODUS network. The TTP and secure billing software will reside on the EXODUS terminal personal computers. A software interface will exist within the EXODUS terminal, which separates ASPeCT and EXODUS functionality. The mobile user will implement some of the TTP and secure billing applications on a smart card. The smart card reader will be connected to the EXODUS terminal via an RS-232 serial interface. The ASPeCT demonstrator software consists partly of commercial applications using Windows Sockets as the interface to the transport protocol. Note that the ASPeCT TTP and secure billing demonstrator and the ASPeCT authentication demonstrator are not to be trialled simultaneously; the user-to-network authentication will be switched off during the TTP and secure billing trial. It is hoped that a first evaluation of the field trial results will be available by the middle of 1998.

On the VASP terminal a WWW server application will provide a value-added information service to trial users. The trial users at the user terminal will use a WWW browser application to retrieve HTML documents that are of particular interest to them using the HTTP protocol. As soon as the browser connects to the server, the ASPeCT payment application on the user terminal will connect to the ASPeCT payment application on the VASP terminal. They will then execute the authentication and initialisation of payment protocol, assuring each other's identity and establishing all the data needed for the charge protocol to be executed and for the on-line credit-based payment of the retrieved information. In the course of this protocol the user's smart card is required. In return for the requested information, the server payment application asks the user for a payment. The user’s payment application responds to this request by making the payment. In the window of the payment application on the user PC and on the VASP PC, all relevant information about the information service and the secure billing protocols associated with the current session are displayed. All this information is also stored in the user’s log file so he can check how much money he spent in all his sessions. The exercise of error conditions and error messages resulting from certificate problems (revoked, out of date etc.) is not included in the trial scenario for the users, but will be included in a separate demonstration.

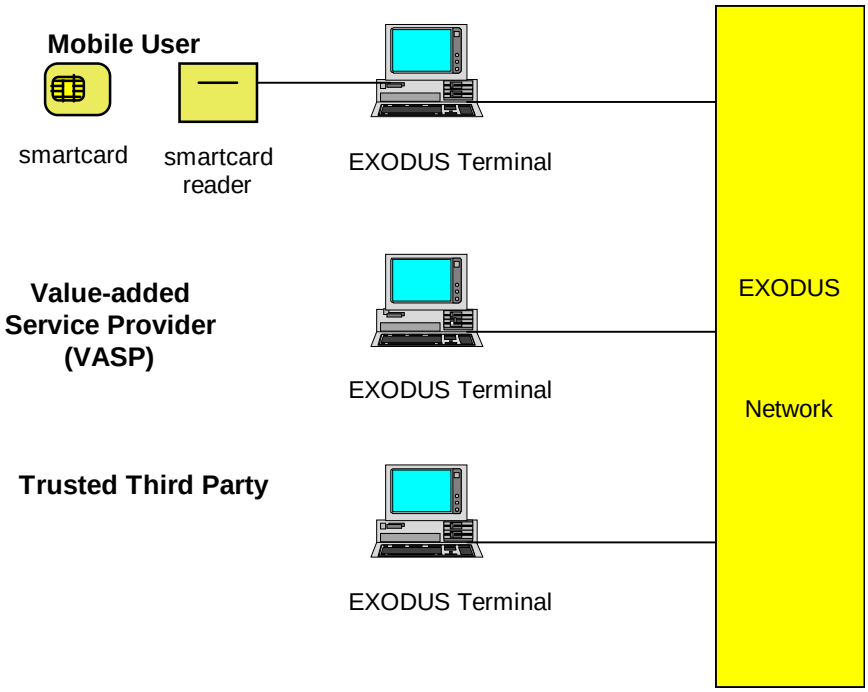


Figure 3: Trial configuration

References

[1] R Anderson, H Manifavas, C Sutherland. A practical electronic cash system. Available from http://www.cl.cam.ac.uk/users/rja14/

[2] A Bosselaers, B Preneel (Eds). Integrity Primitives for Secure Information Systems, Final Report of RACE Integrity Primitives Evaluation (RIPE), R1040, Lecture Notes in Computer Science 1007, 1995.

[3] ETSI SMG SG DOC 73/95, A public key based protocol for UMTS providing mutual authentication and key agreement.

[4] R Hauser, M Steiner, M Waidner. Micro-payments based on iKP. Presented at SECURICOM 96. Available from http://www.zurich.ibm.com

[5] G.Horn and B. Preneel. Authentication and Payment in Future Mobile Systems, Technical Report ESAT-COSIC Report 98-2, Department of Electrical Engineering, Katholieke Universiteit Leuven, Feb., 1998.

[6] ISO/IEC 9796-2. Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Mechanisms using a hash function, 1997.

[7] ISO/IEC FCD 14888-3. Information technology - Security techniques - Digital signature with appendix - Part 3: Certificate-based mechanisms, 1997.

[8] L Lamport. Password authentication with insecure communication. Communications of the ACM, 24 (1981), pp770-772.

[9] K.M.Martin, B.Preneel, C.J.Mitchell, H.J.Hitz, G.Horn, A.Poliakova and P.Howard. Secure Billing for Mobile Information Services in UMTS, to appear in Proceedings of IS&N ’98.

[10] T P Pedersen. Electronic payments of small amounts. DAIMI PB-495, Computer Science Department, Aarhus University, August 1995.

[11] R L Rivest, A Shamir. PayWord and MicroMint: Two simple micropayment schemes. Cryptobytes Vol 2, No 1, pp7-11, May 1996. Available from http://theory.lcs.mit.edu/~rivest

[12] J.Zhou and K.-Y.Lam. Undeniable Billing in Mobile Communication. Preprint, National University of Singapore, March 1998.