A secure GSM-based electronic Murabaha transaction

Mansour A. Al-Meaither and Chris J. Mitchell
Information Security Group, Royal Holloway, University of London
Egham, Surrey, TW20 0EX, United Kingdom
M.Al-Meaither, C.Mitchell@rhul.ac.uk

Abstract

Conventional credit card transactions are not consistent with Islamic principles. In this paper we present a method for mobile secure electronic Murabaha transactions using a combination of the Internet, a GSM mobile device, and a hash-chain scheme related to S/KEY. After introducing the notion of Murabaha sale, we outline the GSM security model and the S/KEY scheme. Security requirements are then identified for a secure GSM-based electronic Murabaha transaction. We then present a protocol designed to address the identified security requirements. Finally, we analyse how the proposed protocol matches the identified security requirements.

1. Introduction

A key concept in the Islamic economic system is the prohibition of payment and receipt of interest on deposits and loans. As a result, Islamic banks offer financial instruments consistent with Islamic religious beliefs, e.g. Murabaha [4].

In recent years, there has been a significant growth in e-commerce transactions that use electronic payment (e-payment) protocols. Although many e-payment protocols have been proposed, only one protocol [1] has been designed to allow electronic commerce transactions based on Islamic banking principles. However, the protocol described in [1] requires the buyer to have a public key pair. This key pair would typically be stored in the buyer PC, and hence the buyer has to use this particular machine every time a transaction is to be made.

Over the last few years, mobile phones have become an essential everyday item for many people, and large numbers of users are reliant on the services that they can provide. The number of mobile phone subscribers worldwide reached 946 million in 2002 [13].

Key characteristics of the mobile phone include the fact that it is ubiquitous, personal, and that the average user is reasonably competent in using it. This fact suggests that it can be used for authentication and authorization in payment transactions since it already contains a physically secure cryptographic device (i.e., the SIM). The combination of a secure subsystem and a familiar user interface means that it also provides a convenient means of generating one-time passwords.

In this paper we present a protocol that combines use of the Global System for Mobile (GSM) infrastructure, a one time password scheme [10], and the Internet, to conduct a secure electronic Murabaha transaction.

After introducing the notion of Murabaha sale, we outline the existing GSM security model. This is followed by a brief description of the S/KEY scheme. Security requirements are then identified for a secure GSM-based Murabaha transaction, followed by a description of the proposed protocol phases. Finally, we analyse how well the proposed protocol meets the identified security requirements, and also show how the approach can be modified to use UMTS instead of GSM.

2. Background

In this section we review the core concepts and technologies underlying our protocol, including the Murabaha sale, GSM air interface security, and the S/KEY scheme.

2.1. Murabaha Sale

Murabaha sale is one of the most commonly used forms of financing provided by Islamic banks. Hasanin [8] notes that Murabaha is the mode of contract most frequently used in Islamic banking, in some cases accounting for 90% of all financing.

A customer wishing to purchase goods requests the Islamic bank to purchase these items on his behalf and then sell them to him, with a certain amount of profit agreed upon added to the initial cost. In the period up to the resale the bank has title to the goods, and hence a legal responsibility. The basic component of Murabaha is that the seller discloses the actual cost he has incurred in acquiring the goods, and then adds some profit thereon.

The validity of a Murabaha transaction depends on certain conditions, which should be properly observed to make the transaction acceptable in Islamic law. The

rules that govern this principle, as stated in [8], are as follows.

- The two sale transactions making up a Murabaha payment, one through which the financial institution acquires the commodity and the other through which it sells it to the customer, should be separate and real transactions.
- The financial institution must own the commodity before it is sold to the customer.
- It is essential to the validity of the Murabaha transaction that the customer is aware of the original price, including the costs necessary to obtain the commodity, and the profit.
- Both parties, i.e. the financial institution and the customer, have to agree on the profit for the financial institution from the sale, where the sum of the cost and profit is equal to the selling price charged by the financial institution.
- It is also necessary for the validity of Murabaha that the commodity is purchased from a third party.

Unless these conditions are fully observed, a Murabaha transaction becomes invalid under Islamic law.

2.2. GSM

Mobile networks conforming to the GSM standards are very widely used worldwide. A GSM network can be divided into three functional entities [14]. These are the mobile station carried by the subscriber, consisting of a Mobile Equipment (ME) with its Subscriber Identity Module (SIM), the network subsystem which performs the switching of calls between the users and between mobile and fixed network users, and the base station subsystem, which controls the air interface between the mobile station and the network subsystem.

The main security services provided by the GSM air interface are, [6, 14]:

- Subscriber identity confidentiality,
- Subscriber identity authentication, and
- Data confidentiality.

Each mobile network operator maintains two databases: the Home Location Register (HLR), and the Visited Location Register (VLR). The HLR is used to store information regarding the subscribers of this operator. The VLR holds information on subscribers which have roamed into its network. GSM air interface security is based on a secret key shared by the subscriber's home network and the SIM. The secret keys of the subscribers are stored in an Authentication Center (AC) which generates security parameters on request by the HLR. The AC is usually implemented as part of the HLR [12].

Each SIM has a unique international mobile subscriber identity (IMSI) and a secret key K_i shared only with the subscriber's network operator AC. During authentication, two keyed functions $(A3, A8)$, and a stream cipher encryption/decryption algorithm $A5$ are used. To authenticate a subscriber (holder of a SIM) to the network, the subscriber sends its IMSI to the VLR, which, in turn, sends a request to the subscriber's HLR. The HLR requests the AC to generate a triplet $(R, SRES, K_c)$, where R is a random challenge, SRES (the expected response to the challenge) $= A3_{K_i}(R)$, and K_c (the session encryption key) $= A8_{K_i}(R)$. The VLR sends R to the SIM which recomputes SRES and K_c using its stored copy of K_i, and returns SRES. If the returned value agrees with the value in the triple, the mobile is deemed authentic, and data exchanged between the mobile and the network is subsequently encrypted using K_c. This encrypted channel is also used to transfer a temporary identity (TMSI) for the mobile, to provide a measure of mobile anonymity.

The SIM Application Toolkit [5] has been proposed as a means of expanding the ME functionality by allowing the addition of applications to the SIM card. The SIM Toolkit specifies an interface between the ME and the SIM, and defines how an application program running on the SIM can register menu elements and listen to events such as the receipt of an SMS message. When an event occurs, a procedure on the SIM is executed. The procedure can invoke other functions of the ME; for example it can display a message, ask for input, or send an SMS.

2.3. S/KEY

S/KEY is a one-time password scheme which has been published as an Internet RFC [7], and is based on a scheme originally proposed by Lamport, [9]. It uses 'one-time passwords' to control user access to a remote host.

In the S/KEY scheme, the user and the host which the user wishes to access share a one-way hash function f. The user first selects a password p. The host is assigned an initial seed value d and a count value c which defines the number of user authentications to be allowed using this seed value. In addition, the host is given the verifier $f^c(s)$ for subsequent authentication, where s is the result of the bit-wise exclusive-or of the user secret password p with d, i.e. $s = p \oplus d$. When the user identity is to be verified, the following procedure is followed.

1. The host decrements its stored counter c for that user and sends the new value of c to the user in conjunction with the seed value d.

2. On receipt of d and c, the user employs his secret password p to compute $f^c(s)$, and sends this value back to the host.

3. On receipt of $f^c(s)$, the host computes $f(f^c(s))$ and compares the result with its stored verifier $f^{c+1}(s)$. If the two values agree then the user is authenticated and the 'old' stored verifier is replaced with $f^c(s)$. Otherwise the user is rejected.

An advantage of the S/KEY scheme is that it does not requires the host to store secret information about the remote user, since it only keeps the 'old' verifier, from which the new verifier (and the secret password p) cannot easily be derived. However, note that, if p is poorly chosen, then knowledge of $f^c(s)$, c and d can be used as the basis of an exhaustive search for p. Also, S/KEY should only be used where the user can be confident of the host identity, otherwise attacks are possible [11].

3. The GSM-based electronic Murabaha transaction model

In this section, we describe our model of a GSM-based electronic Murabaha transaction, in which the Internet and the GSM security infrastructure are combined to enhance electronic Murabaha transaction security and provide buyer mobility. The entities involved, and their interactions, are described and the security requirements are listed.

3.1. Entities involved

The GSM-based electronic Murabaha transaction defined here involves interactions between four parties: the buyer, the merchant, a GSM Authentication Centre, and the provider.

- **Buyer**: This is the entity that wishes to buy goods from a merchant via the Internet, but does not have the cash immediately available to complete the transaction. The buyer must have access to the Internet and a SIM Application Toolkit compliant mobile phone. It is assumed that the SIM in the buyer mobile phone contains a SIM Toolkit compliant payment application.

- **Merchant**: This is the entity that offers the goods for sale (via the Internet) which the buyer wishes to purchase. We assume that the communications link between the provider and the merchant offers confidentiality, integrity, and origin authentication, for example as provided by the Transport Layer Security (TLS) protocol [3] with both client and server authentication.

- **Provider**: This is a financial institution that acts as an intermediary between the buyer and the merchant. It undertakes the purchase of commodities as specified by a buyer, and then resells them on a Murabaha basis to him for the cost price plus a margin of profit agreed upon previously by the two parties. It does not make a purchase unless the buyer both requests it and makes a prior promise to purchase. It is assumed that the provider has a contractual agreement with the mobile network operator to regulate the relationship. In order to communicate with the buyer, the provider has a GSM-enabled device (with a SIM) via which it can send and receive SMS messages; it is further assumed that the SIM is issued by the same network operator that issued the buyer's SIM, and contains an appropriate SIM toolkit compliant payment application. Moreover, we assume that the buyer trusts the provider. This trust is explicit as the buyer is assumed to have a formally established agreement with the provider that defines the trust and liability relationship.

- **Authentication Centre**: This is the AC belonging to the GSM mobile network operator shared by the buyer and the provider. In our protocol it is used as a key distribution centre, where it receives requests from the provider to generate a session key used to secure communications between the buyer and the provider. We assume that the communications link between the provider and the AC offers confidentiality, integrity, and origin authentication, for example as provided by TLS with both client and server authentication.

3.2. Interaction

In the proposed transaction, the buyer shopping at an Internet merchant site first chooses to pay using Murabaha through a specified provider. The merchant contacts the selected provider to complete the transaction. If the provider chooses to proceed with the transaction, he calculates his profit and sends the buyer an SMS message promising to sell the goods to the buyer. In return, the buyer replies with an SMS message in which the buyer promises to buy the goods on a Murabaha basis for the cost of the goods plus the agreed upon profit. This promise is not binding on either the buyer or the provider, and is not an actual sale. At this stage the relationship between the buyer and the provider is that of promisor and promisee. Based on the response received from the buyer, the provider communicates with the merchant Internet site and completes the purchase of the goods. One possible additional benefit of this procedure is that the provider is in a better position to obtain discounts from the merchant, who in most cases will prefer dealing with a provider, as the merchant will receive

payment more quickly and with less risk. Once the purchase of the goods is settled between the provider and the merchant, the provider sends an SMS message to notify the buyer of completion of the purchase and offer him the goods. If the buyer agrees, he sends his payment authorisation back to the provider (an SMS message) to buy the goods from the provider on a Murabaha basis. The provider asks the merchant to deliver the goods to the buyer.

3.3. Security requirements

In this section we identify what security services are required for a secure GSM-based electronic Murabaha transaction. The security services can be divided into four categories: authentication, confidentiality, integrity, and non-repudiation.

3.3.1. Authentication

In the context of the proposed protocol, this security service can be sub-divided into the following:

1. Verification by the provider that the merchant and the AC are as claimed.
2. Verification by the buyer that the provider is as claimed.
3. The provider needs to be sure that the buyer is the legitimate owner of the SIM and that the source of the payment authorisation is a legitimate SIM.

3.3.2. Confidentiality

This security service can be sub-divided into the following:

1. The buyer authorisation must be kept secret from non-authorised parties.
2. The buyer may require privacy of his order information.

3.3.3. Integrity

This security service can be sub-divided into the following.

1. The buyer must be aware of the original price of the goods being purchased and the amount of profit the provider is charging him before buying the goods. This is necessary if the transaction is to be compatible with Murabaha sale conditions.
2. The buyer requires assurance that the provider owns the goods being offered.
3. The transaction data communicated between the participants should be protected against modification and replay.
4. The buyer payment authorisation must be protected against alteration, or any alteration must at least be detectable.

3.3.4. Non-repudiation

In the context of our transaction model, the provider must possess evidence that the buyer has authorised payment for the goods on a Murabaha basis. This proof must not be replayable, or usable as proof for some other transaction.

4. The protocol

We now describe the proposed GSM-based electronic Murabaha transaction in detail. The protocol consists of five phases: the *Registration phase*, in which the buyer sets up an S/KEY system with the provider; the *Transaction request phase*, in which the buyer finds goods he wishes to buy at an Internet merchant site, and decides to use Murabaha to pay for the goods; the *Confirmation phase*, invoked by the provider, wherein the provider promises to sell the buyer the goods he is interested in, while the buyer promises to buy the goods from the provider, once the provider has ownership; the *Purchase phase*, invoked by the provider, wherein he buys the goods requested by the buyer from the merchant, and the *Murabaha phase*, invoked by the provider, wherein the buyer validates the provider's ownership of the goods offered and sends authorisation to the provider to buy the goods at the agreed price.

The transaction is based on a combination of secret key encryption, computation and verification of Message Authentication Codes (MACs), and a hash-chain scheme related to S/KEY. The provider needs to store one time passwords (hash values) released by the buyer as evidence that the buyer authorised the Murabaha transaction.

In the protocol descriptions we make use of the following notation.

- B: the buyer,
- c: the number of buyer authentications remaining before the S/KEY system needs to be re-initialised,
- d: the initial seed value used in the S/KEY system,
- $E_K(M)$: the encryption of message M (using symmetric encryption) with key K,
- f: a one-way hash function,

- $\text{MAC}_K(M)$: a MAC computed on message M using a variant of key K (note that it is important that the key used to compute the MAC is not precisely the same as the key used for encryption, particularly if the MAC is a CBC-MAC [10]),
- MN: the buyer mobile number,
- p: the buyer secret password,
- P: the provider,
- PI: the Purchase Information,
- R_i: a random nonce generated by entity i,
- $X||Y$: the concatenation of data items X and Y, and
- $\oplus$: the bitwise XOR operation.

4.1. Registration

Initially, the provider and the buyer mobile (in fact the SIM) sets up an S/KEY system by means of a secure channel. The one-way hash-function f must also be agreed.

- The buyer invokes his SIM Toolkit payment application, inputs his own secret password p, and inputs the value of c selected by the provider; the application selects a random value for d.
- The SIM Toolkit payment application computes $s = p \oplus d$, and $f^c(s)$, where f^c is the recursive application of f a total of c times, and securely transfers $f^c(s), c$ and d to the provider for subsequent Murabaha transaction authorisations.

After the allowed number of buyer authentications c has expired, the buyer is expected to re-initialise the S/KEY system using the steps described above. The provider selection of the value of c must take into account the level of risk that he is willing to take.

4.2. Transaction request

This phase begins when a buyer, shopping at an Internet merchant site, indicates that he wishes to make a specific purchase using Murabaha through a specified provider, and fills in an Internet form that contains a field for a GSM phone number and a random number. The buyer invokes the SIM Toolkit payment application in his mobile phone, which, in turn, generates and displays a random number R_B. The buyer enters R_B and his mobile number MN in the merchant form. On receipt of the form, the merchant prepares a quotation that contains data related to the goods being offered, such as the goods description, price, validity of the quotation, MN and R_B. After preparing the quotation, the merchant sends it to the specified provider in order to finalize the transaction. This quotation is optionally signed by the merchant. We assume that the merchant and the provider are using appropriate security measures that provide entity authentication and integrity protection to protect messages exchanged during the course of the transaction.

4.3. Confirmation

In this phase, both the provider and the buyer use the GSM security infrastructure to establish a shared secret session key, which they can use to provide security for the rest of the transaction. Moreover, the provider starts to negotiate with the buyer to assert his willingness to buy the goods specified in the previous phase.

1. $P \rightarrow AC : MN$
2. $AC : K_s = A8_{K_i}(R_{AC})$
3. $AC \rightarrow P : R_{AC}||K_s||MN$
4. $P \rightarrow B :$
   $R_{AC}||E_{K_s}(PI||R_B||\text{Trans\_Id})||\text{MAC}_{K_s}(PI||R_B||\text{Trans\_Id})$
5. $B \rightarrow P :$
   $E_{K_s}(PI||\text{Trans\_Id}||Y/N)||\text{MAC}_{K_s}(PI||\text{Trans\_Id}||Y/N)$

Upon receipt of the quotation prepared in the transaction request phase and successfully verifying the merchant's signature, the provider sends a session key request to the AC, as shown in step 1. The request contains the buyer mobile number MN. The AC retrieves the buyer shared secret key K_i corresponding to the MN and uses it, along with a new random number R_{AC}, to derive a random session key K_s for this transaction (step 2).

The AC then constructs and sends a response message to the provider (step 3). This message contains the random number R_{AC} used to generate the session key K_s, the buyer mobile number MN.

After receiving the message in step 3, the provider constructs the Purchase Information (PI), which contains an abbreviated goods description, the cost of the goods to the provider, the profit requested by him, and the date the provider expects the buyer payment. The inclusion of the profit requested by the provider is to satisfy the conditions set out in 2.1. The provider then creates and sends an SMS message that contains R_{AC} and a promise to sell the requested goods to the buyer once they have been bought from the merchant (step 4). The promise includes the PI, the random number R_B received in the transaction request, and a Transaction Identification number (Trans_Id) chosen by the provider to uniquely identify the context. The provider encrypts the promise using the session key K_s.

A MAC is also computed on the promise to sell message using the key K_s. The enciphered information and the MAC are then sent to the buyer. It should be noted that the key used to compute the MAC is not precisely the same as the key used for encryption; we assume that the encryption and MAC functions use different keys derived from K_s.

Upon receipt of the SMS message in step 4, the SIM Toolkit payment application in the buyer SIM calculates the key K_s using the received R_{AC} and the SIM stored key K_i as inputs to the key derivation algorithm $A8$ shared with the AC, i.e. $K_s = A8_{K_i}(R_{AC})$.

The buyer then decrypts the promise to sell and verifies the MAC to check message integrity using K_s. If the MAC is valid, then the provider must possess the same session key K_s.

The buyer then checks that the goods promised by the provider are the requested goods. Also, the buyer checks that both the profit and the due date offered by the provider are acceptable to him. If the buyer chooses to proceed with sale, then he responds to the provider with a promise to buy SMS message (step 5) to indicates to his willingness to buy the goods once the provider has the ownership of them. The message includes the PI, the Trans_Id, and B's agreement to continue the transaction (Y/N), encrypted and MACed using K_s.

4.4. Purchase

When the provider receives the promise to buy SMS message from the buyer (step 5 of the confirmation phase), he decrypts it using the shared session key K_s and checks that the contents are as expected. Then, the provider verifies the MAC on the message using K_s. If the MAC is valid then the provider completes the purchase of the goods from the merchant. We assume that the provider signs a message that guarantees the merchant payment. Once the merchant has verified the promise of payment for the goods from the provider, the merchant displays a message to the buyer confirming that the transfer of goods to the provider has taken place. This gives the buyer assurance that the provider has purchased the goods, and also serves as a prompt to the buyer to purchase the goods from the provider.

4.5. Murabaha

In this final phase the buyer purchases the goods from the provider. The two messages below are both sent as SMS messages.

1. $B \rightarrow P$:
   $E_{K_s}(PI||\text{Trans\_Id}||f^{c-1}(s))||\text{MAC}_{K_s}(PI||\text{Trans\_Id}||f^{c-1}(s))$
2. $P \rightarrow B$:
   $E_{K_s}(\text{Trans\_Id}||f^{c-1}(s))||\text{MAC}_{K_s}(\text{Trans\_Id}||f^{c-1}(s))$

If the buyer chooses to complete the transaction, then he constructs and sends a payment authorization to the provider as shown in step 1. The payment authorization contains PI and Trans_ID. Moreover, it contains the current value in the password chain ($f^{c-1}(s)$) which confirms the buyer agreement to buy the goods on a Murabaha basis. To ensure that only the rightful owner of the phone can generate the authorisation, the SIM Toolkit payment application can additionally ask the buyer to identify himself before sending this message, e.g. using a PIN; the application then sends the payment authorisation to the provider.

Upon receipt of the message in step 1, the provider uses the one way function f to check whether $f(f^{c-1}(s)) = f^c(s)$. If the check succeeds, then the provider saves the current $f^{c-1}(s)$ as an evidence of the transaction authorisation, decrements c, and updates $f^c(s)$ with $f^{c-1}(s)$. If the provider does not receive $f^{c-1}(s)$, or receives incorrect $f^{c-1}(s)$, then the provider terminates the transaction.

After correct verification of the buyer authorisation, the provider instructs the merchant to dispatch the goods to the buyer address (which is already known to the provider at registration). Moreover, the provider sends a completion message to the buyer (step 2). Upon receiving the message in step 2, the buyer SIM Toolkit payment application decrypts $E_{K_s}(\text{Trans\_Id}||f^{c-1}(s))$. If the data is as expected and the MAC verifies correctly, then the buyer SIM Toolkit payment application decrements c, and ends the application.

5. Security Analysis

In this section, we examine to what extent the generic security requirements outlined in section 3.3 are met by the proposed transaction.

5.1. Authentication

1. *Verification by the provider that the merchant and the AC are as claimed.* In the proposed transaction, it is assumed that the provider is using a security protocol such as TLS to authenticate both the merchant and the AC.

2. *Verification by the buyer that the provider is as claimed.* If the buyer can verify the MAC received in message 4, then this implies the freshness of the transaction because the message contains the PI, R_B and a Trans_ID. Therefore, the buyer has authenticated the provider. However, because R_{AC} is not authenticated then there is a possibility that the MAC has been generated using an old R_{AC} with a compromised K_s.

On the other hand, the buyer SIM communication with the provider is based on the key K_s generated by the AC. The assumption here is that the provider receives a trusted copy of the K_s using a secure channel between the AC and the provider. Therefore, unless the provider has the correct K_s he will not be able to continue the transaction.

3. *The provider needs to be sure that the buyer is the legitimate owner of the SIM and that the source of the payment authorisation is a legitimate SIM.* A legitimate owner of the SIM will need to enter the correct PIN to use it. Even if an attacker has stolen the SIM and impersonates the buyer to purchase goods, he will not be able to gain financially because the goods will be delivered to the buyer address registered in the provider database. The proposed transaction does not prevent this attack unless the buyer SIM is reported stolen and blocked by the mobile network operator, although this will normally occur, since the SIM holder will wish to avoid paying for calls made using a stolen SIM. Moreover, the payment authorisation sent in step 1 of the Murabaha phase is generated using a key K_s shared between the buyer and the provider. The key K_s can only be generated by a SIM that has the correct key K_i.

5.2. Confidentiality

1. *The buyer authorisation must be kept secret from non-authorised parties.* The value $f^{c-1}(s)$ generated by the buyer is sent to the provider in an encrypted SMS message. The encryption key used is known only to the buyer, the provider and the AC. The AC is trusted not to reveal the key and hence $f^{c-1}(s)$ will not be available to unauthorised parties. Furthermore, the value $f^{c-1}(s)$ is used only once.

2. *The buyer may require privacy of his order information.* All messages exchanged between the buyer and the provider are encrypted using a shared session key. An advantage of our transaction scheme is that the buyer does not need to send any private information via the merchant, unlike conventional e-commerce schemes where a credit card number is sent to a merchant protected using TLS. This avoids any concerns regarding the ability of the merchant to store buyer private information in a secure manner. However, the buyer will need to provide the MN and R_B to the merchant via the purchase form. This information is sent to the provider using a secure channel, e.g. as provided using TLS.

5.3. Integrity

1. *The buyer must be aware of the original price of the goods being purchased and the amount of profit the provider is charging him before buying the goods.* This requirement is met, because in order for the provider to complete the transaction, the buyer must respond to the message sent in step 4 of the confirmation phase. If the buyer replies with the message in step 5 then he must know the original price and the amount of profit the provider is adding, since it is included in the PI.

2. *The buyer requires assurance that the provider owns the goods being offered.* We assume that the merchant, once it has sold the goods to the provider, will display a message to the buyer indicating the transfer of the goods ownership to the provider. However, this is not verifiable by the buyer.

3. *The transaction data communicated between the participants should be protected against modification and replay.* While the communication link between the AC and the provider is assumed to be secure, the AC is using SMS messages to communicate with the buyer SIM. If an attacker modified the R_{AC} sent by the AC to the buyer SIM, then the SIM will generate a different session key from the one AC would send to the provider. Therefore, the buyer SIM and the provider will not be able to establish a secure channel.

   On the other hand, an attacker can force re-use of an old R_{AC} for which the corresponding key K_s is known. It is therefore important for the AC to use numbers with good randomness properties, such that the probability of sending the same R_{AC} twice to the buyer SIM is negligible.

4. *The buyer payment authorisation must be protected against alteration, or any alteration must be detectable.* The payment authorisation sent in step 1 of the Murabaha phase is protected against unauthorised modification through the use of a MAC. Without the key K_s, it is assumed to be infeasible to generate a valid MAC for a modified authorisation message

5.4. Non-repudiation

The provider must possess evidence that the buyer has authorised payment for the goods on a Murabaha basis.

The one way function f is used to achieve non-repudiation. In the ith session, the buyer provides $f^{c-i}(s)$ to authorise the Murabaha transaction. The provider can verify the correctness of $f^{c-i}(s)$ but cannot derive $f^{c-i}(s)$. from $f^{c-i+1}(s)$. Therefore, $f^{c-i}(s)$ can

be used as evidence of the ith authorisation. Moreover, the buyer buyer authorisation $f^{c-i}(s)$ is different for each transaction, and therefore $f^{c-i}(s)$ is not replayable, or usable as proof for some other transaction.

6. UMTS/3GPP extension

In this section we describe a way in which the proposed protocol can be extended to utilise the security services offered by the Universal Mobile Telecommunications System (UMTS) of the Third Generation Partnership Project (3GPP).

In addition to the security services already provided by the GSM air interface, UMTS offers the following enhancements, [2]:

- Mutual authentication between the user and network.
- Assurance that authentication information and keys are not being re-used.
- Integrity protection of signalling messages.
- Use of stronger encryption.

As in GSM, UMTS security is based on a secret key K shared between a User Services Identity Module (USIM), and the network operator's AC. In addition, UMTS uses a set of predefined cryptographic functions '$f1 - f5$' to generate the security parameters needed during the authentication and key agreement procedures. For example, $f1$ is a message authentication function, $f3$ is a key generating function used to generate a cipher key CK and $f4$ is key generating function used to generate an integrity key IK.

Our protocol can be adapted to take advantage of the UMTS security features. Specifically, $f1$ can be used to generate the necessary MACs and $f3$ can be used to generate the session key K_s. Moreover, the integrity key IK can be used instead of using a variant of the session key K_s to compute the MAC.

7. Conclusion

In this paper we have a proposed a secure GSM-based electronic Murabaha payment protocol where the GSM infrastructure is used in authentication and payment authorisation. In addition to the Internet, the scheme uses SIMs equipped with a special SIM Toolkit payment application. We have described the scheme in detail, explained how it meets the identified security requirements and showed how it can be extended to use UMTS/3GPP security features.

References

[1] M. Al-Meaither and C. J. Mitchell. A secure electronic Murabaha transaction. In *Proceedings of eTransformation, 16th Bled eCommerce Conference*, pages 662–674, Bled, Slovenia, University of Maribor, June 2003.

[2] C. W. Blanchard. Security for the third generation 3G mobile system. *Information Security Technical Report*, 5(3):55–65, 2000.

[3] T. Dierks and E. Rescorla. *The TLS Protocol Version 1.0*. Certicom, January 1999. Internet RFC 2246.

[4] Mahmoud Amin El-Gamal. A basic guide to contemporary islamic banking and finance, 2000. http://www.ruf.rice.edu/~ elgamal/files/primer.pdf.

[5] European Telecommunications Standards Institution (ETSI). *Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit (SAT) for the Subscriber Identity Module - Mobile Equipment (SIM-ME) Interface (3GPP TS 11.14 version 8.14.0)*, June 2003.

[6] European Telecommunications Standards Institution (ETSI). *Digital cellular telecommunications system (Phase 2+); GSM Security Aspects (GSM 02.09 version 8.0.1)*, June 2001.

[7] N. Haller. *The S/KEY one-time password system*. Bellcore, February 1995. Internet RFC 1760.

[8] Fayad Hasanin. *Murabaha Sale in Islamic Banks*. The International Institute of Islamic Thought, Herndon, VA, U.S.A, 1996.

[9] Leslie Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11):770–772, 1981.

[10] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of applied cryptography*. CRC Press, Boca Raton, FL, USA, 1997.

[11] C. J. Mitchell and L. Chen. Comments on the S/KEY user authentication scheme. *ACM Operating Systems Review*, 30(4):12–16, 1996.

[12] S. M. Redl, M. K. Weber, and M. W. Oliphant. *An Introduction to GSM*. Artech House, Norwood, MA, U.S.A, 1995.

[13] International Telecommunication Union. The mobile revolution — World trends internet for mobile generation, 2002. http://www.itu.int/itunews/.

[14] M. Walker and T. Wright. Security. In F. Hillebrand, editor, *GSM and UMTS: The creation of global mobile communication*, chapter 14, pages 385–406. John Wiley & Sons, 2002.