Development and Performance Evaluation of a Mobile Banking System based on the HBCI Standard

Ian Herwono
Chair of Communication Networks
Aachen University of Technology
Kopernikusstr. 16, D-52074 Aachen, Germany
ian@comnets.rwth-aachen.de

Abstract

The introduction of *Wireless Application Protocol (WAP)* as the key technology to access the Internet from cellular phones opens new business opportunities for service and content providers. Among such *Mobile Commerce* (m-commerce) services, mobile banking (m-banking) service was rated as the top application demanded by more than 85 % of potential users in Europe [4]. This paper presents a novel concept of mobile banking system which is based on the German home-banking standard *HBCI*. The concept considers the typical characteristics of cellular systems, such as limited bandwidth or user interface capability, while still being conform to the banking standard, e.g., regarding its security measures. A simulation system is developed to estimate the performance of the elaborated transaction protocols and employed cryptographic algorithms regarding their time behaviors. The performance of an example scenario for portfolio order transaction is estimated.

1. Introduction

The mobile market was growing steadily in the recent years, and so did the user acceptance of mobile devices. For example, in Germany, there are now more people using cellular phones than the Internet. Getting access to bank account or portfolio from home by using a PC (home-banking) will become more and more common for each individual. Hence, the market of cellular phone users and mobile financial services overlap. This encourages the mobile operators and financial institutions to look for a solution that combines secure account management with mobile devices.

Existing banking and cellular standards have to be investigated regarding their usability and applicability for such a solution. The German *Home Banking Computer Interface (HBCI)* is a banking standard which allows secure financial transactions to be carried out on public (insecure) networks, such as the Internet. HBCI provides the customers with a secure access to their bank accounts or portfolios. Since HBCI is an open standard, mobile operators or service providers would be able to offer their customers access to all banks that support HBCI, without having to implement different protocols for each bank.

The *Wireless Application Protocol (WAP)* is an open standard aiming at providing cellular phones with a common access to the Internet. In combination with common cellular standards like the GSM[1], WAP would be a key technology for secure mobile financial solutions. The WAP security protocol can be used to interchange data securely between mobile devices and m-commerce (*Mobile Commerce*) servers that may be located within the cellular network infrastructure.

The harmonization of both standards, the banking and the cellular standards, is essential for the success of a mobile financial service. This is due to the fact that the methods and protocols defined in existing banking standards may not be applied directly within cellular systems, since such issues like limited bandwidth, more error-prone mobile channels, or limited user interface capability (small display), have to be considered.

In this work, a solution for a mobile financial service that is based on the HBCI standard is developed and evaluated. The work focuses on the realization of a mobile brokerage system where customers can sell or buy stocks by using their mobile devices. The system can be extended to other typical banking transactions, such as funds transfer or balance inquiry.

2. Home Banking Computer Interface

2.1. Overview

The *Home Banking Computer Interface (HBCI)* [1] is an open home-banking standard that will be supported by all banks and financial institutions in Germany soon. The international standardization of HBCI is also planned. HBCI provides a multi-bank capable interface between customer products and bank systems, i.e., it allows a customer to manage his/her accounts at several banks by using a single client software. In addition, HBCI is independent of the used transport medium and end devices. In its current version 2.1, typical banking transactions belonging to the following categories are specified:

[1] Global System for Mobile Communications

- domestic and international payments,
- account movements information,
- time deposits,
- portfolio order,
- ordering of bank cards, checks and forms.

Other business cases and functions will be gradually added to HBCI. The next version will include travelers' checks and foreign currency orders, single transaction queries and electronic wallet recharging.

2.2. HBCI Message Structure

HBCI makes use of the international ISO 8859 standard character set for all of its texts and messages which will be interchanged between client (customer product) and server (bank system). The language-specific subset of ISO 8859 is also supported. The messages may also contain binary information which is represented in a standardized bank-specific format, such as S.W.I.F.T.[2] MT502 data format. Separator character syntax is used, along with a release character. Optional data fields are marked as such and included at the end of the data structure.

In general, an HBCI message consists of several data segments. A message always begins with a header segment (HNHBK) and ends with a message terminator segment (HNHBS). The header is followed by a signature header (HNSHK), HBCI user data, and a signature terminator (HNSHA). In case of an encrypted HBCI message, the header segment is followed by an encryption header segment (HNVSK), which is in turn followed by an encrypted data segment that consists of signature header, user data and signature terminator (**Fig. 1**).

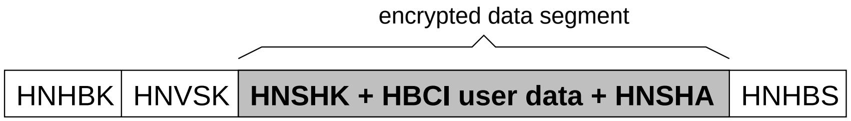

Fig. 1 General HBCI message structure

2.3. HBCI Session

HBCI messages are interchanged between client (customer) and server (bank) within a synchronous HBCI session, i.e., each client request message must be responded by the HBCI server, as shown in **Fig. 2**. An HBCI session is divided into three phases. First, a session initialization is performed. In this phase, a mutual user authentication between customer and bank is carried out. In the second phase, transaction messages are interchanged securely. Finally, the session is terminated in the last phase. As depicted in **Fig. 2**, more than one business transaction can be performed within a single HBCI session.

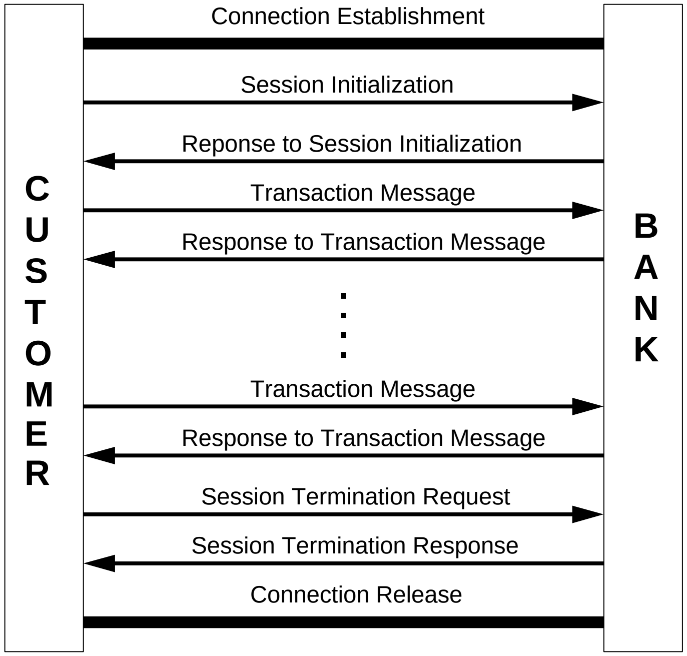
CUSTOMER
BANK
Connection Establishment
Session Initialization
Reponse to Session Initialization
Transaction Message
Response to Transaction Message
Transaction Message
Response to Transaction Message
Session Termination Request
Session Termination Response
Connection Release

Fig. 2 A single HBCI session

2.4. HBCI Security

Since HBCI was designed for the usage within public (insecure) network environments, extensive security measures have been specified in the standard.

[2] Society for Worldwide Interbanking Financial Communication

These regard both the enciphering and signing of transaction messages. Two security procedures are in use within the HBCI framework:

- a chip card procedure based on the symmetric DES[3] procedure, and
- a procedure based on the asymmetric RSA[4] procedure.

The two procedures are designated respectively DDV (DES/DES Procedure), and RDH (RSA/DES Hybrid Procedure). DDV uses a MAC[5] as signature and encrypts the message key with 2-key Triple-DES algorithm, whereas RDH signs the messages and encrypts the message key with RSA. Ultimately, it is intended to use the RSA procedure combined with a chip-card for all security solutions, based on current RDH specifications.

3. Wireless Application Protocol

The *Wireless Application Protocol (WAP)* [5] specifies an application framework and network protocols for wireless devices, such as cellular phones, pagers, and personal digital assistants (PDAs). It is positioned at the convergence of two rapidly evolving network technologies, i.e., wireless data and the Internet. In order to provide users with Internet-like (IP based) services, the WAP specifications address cellular system characteristics and operator needs by adapting existing network technology to the special requirements of mass market, handheld wireless devices and by introducing new technology where appropriate. This process of specification is presently going on and newer versions of the WAP protocol stack show an increasingly sophisticated approach towards bringing the two network technologies together. The WAP protocol stack consists of the following six layers:

- Wireless Application Environment (WAE)
- Wireless Session Protocol (WSP)
- Wireless Transaction Protocol (WTP)
- Wireless Transport Layer Security (WTLS)
- Wireless Datagram Protocol (WDP)
- Adaptation layer for specific bearer services

WAP enables a flexible security infrastructure that focuses on providing connection security between a WAP client and a WAP server[6]. WAP can provide end-to-end security between WAP protocol endpoints by using its SSL[7]-like WTLS protocol. If a browser and origin server desire end-to-end security, they must communicate directly using the WAP protocols.

4. Mobile HBCI Concept

The objective of Mobile HBCI is to satisfy the following requirements for a mobile client (software/hardware) to carry out HBCI transactions:

- The client should be able to support various business transactions.
- The business transactions should be configurable from the server, e.g., for version management.
- The type and amount of transaction data that is to be entered by the user on the client manually, should be suited to the (limited) capability of the client's user interface, i.e., small display, limited keypad.
- Since the customer's private signature key is stored on chip-card, the signing procedure should be carried out on the mobile device.

The concept introduces the use of an intermediate server, called *HBCI agent*, that is logically located between the cellular system (including the WAP proxy/server) and the bank system (**Fig. 3**). Within a Mobile HBCI session, the mobile client communicates only with the HBCI agent, which in turn processes the HBCI transactions and communicates with the bank's HBCI server (via the Internet or banking network) on behalf of the client (customer). Since the HBCI agent doesn't own the client's private keys, the agent is thus not capable to generate and send a complete (authorized) HBCI messages to the HBCI server by itself.

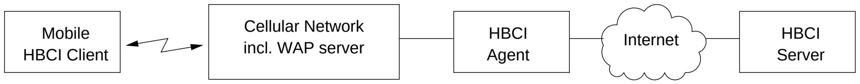

Fig. 3 Mobile HBCI system architecture

[3] Data Encryption Standard
[4] Rivest Shamir Adleman
[5] Message Authentication Code
[6] also known as WAP gateway
[7] Secure Socket Layer

4.1. Mobile HBCI Session

Mobile HBCI session conforms to the standardized HBCI session. According to the standard, the messages used for session initialization and termination have to be generated by the client. Hence, the main part of Mobile HBCI is the HBCI agent and its communication procedures with mobile client (customer) and HBCI server (bank). An overview of a Mobile HBCI session is given in **Fig. 4**.

After the customer has entered the transaction data into the mobile device and initiated the transaction, the client establishes a connection to the HBCI agent through the WAP server via the radio interface. Then, the HBCI agent sets up a connection with the corresponding HBCI server. The establishment of a secure WAP data connection, i.e., a WTLS-secured connection, is optional, since WTLS only secures the connection between client and WAP server, not between client and HBCI agent. Hence, Mobile HBCI defines application-specific security procedures to provide end-to-end security between client, HBCI agent and HBCI server. After the connection is established, the HBCI session initialization procedure can be started by the client.

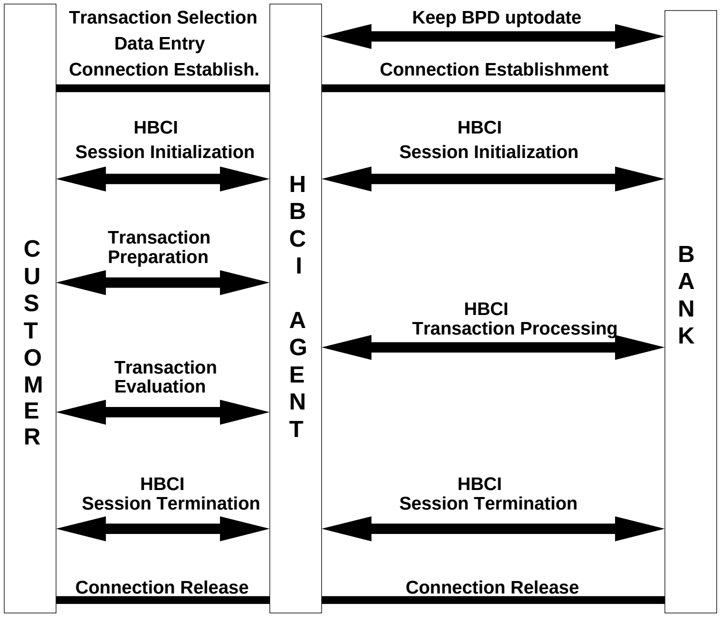

Fig. 4 Mobile HBCI session

4.2. Communication between Client and Agent

4.2.1. Secure User Data Interchange

Interchange of user data between mobile client and HBCI agent is carried out after a session initialization procedure succeeded. In order to ensure the integrity of the data transmitted via the radio interface and WAP gateway, the transaction messages are signed by the client or agent using RSA procedure. The user (transaction) data is enciphered with a message (session) cipher key by using Triple-DES algorithm which is operating in CBC[8] mode. The session cipher key is randomly generated within the client's security module, e.g., a chip-card. **Fig. 5** depicts the whole signing and enciphering procedure within a secure user data interchange procedure in case that a message is to be transferred from client to agent. At the agent's side, the interchanged message is deciphered, and its signature is verified.

4.2.2. HBCI Hash Value

After deciphering and verifying the interchanged user data, the HBCI agent assembles the corresponding HBCI message segments and generates the signature header (HNSHK). Then, a hash value is calculated over the particular HBCI segments by using RIPEMD160 hash algorithm. According to the specification, the segments are the signature header and the HBCI user data[9].

Since each HBCI transaction must be signed by the customer (client) and the HBCI agent doesn't own the required private signature key, the HBCI hash value must be sent back to the mobile client first. The client calculates the signature by using RSA procedure and encrypts both the signature and the hash value with a session cipher key by using Triple-DES algorithm (CBC mode). Then, it sends the result to the agent according to procedure depicted in **Fig. 5**.

4.2.3. Transport of HBCI Message Cipher Key to Agent

In order to allow the HBCI agent to send a complete ciphered HBCI message to the HBCI server, the HBCI message cipher key[10] must be sent from the client to

[8] Cipher Block Chaining

[9] Note that the HBCI user data is not identical with the user data interchanged via the radio interface.

[10] Note that the HBCI message cipher key is not identical to the message cipher key used in the user data interchange procedure depicted in **Fig. 5**.

the agent first. According to HBCI standard, the message cipher key has to be re-generated by the client for each HBCI message. **Fig. 6** illustrates the HBCI message encryption procedure using the message cipher key (performed by the agent).

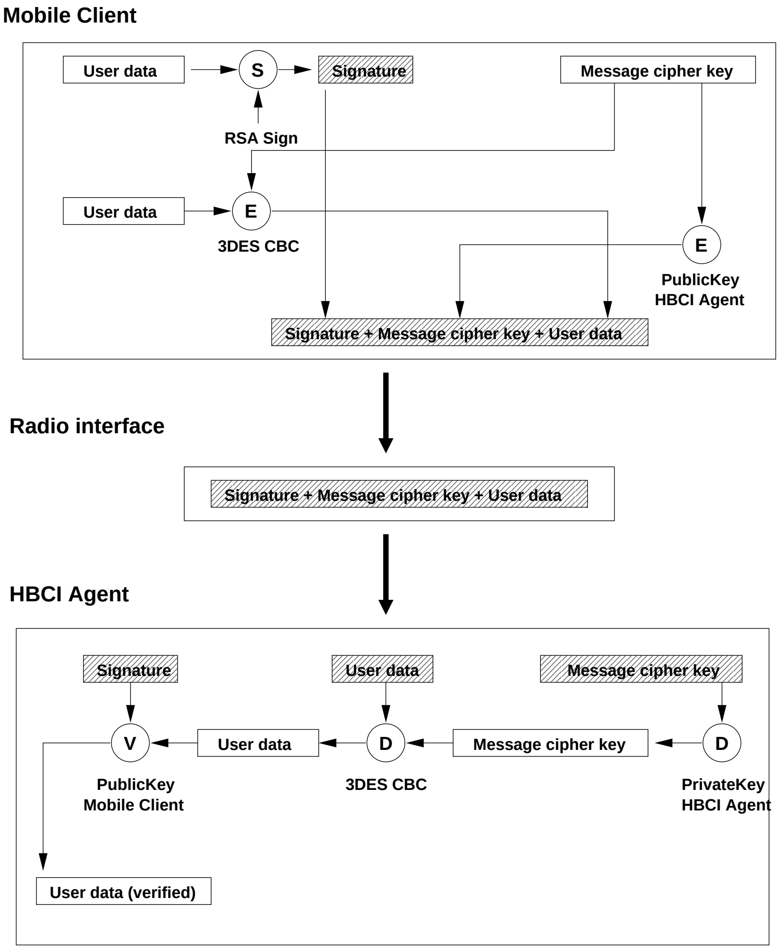

Fig. 5 Secure user data interchange procedure

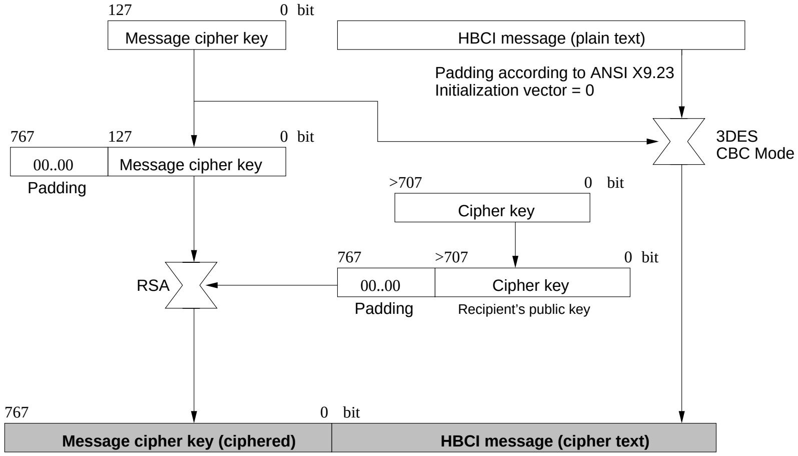

Fig. 6 Standard HBCI message encryption

4.2.4. Interchange of HBCI Messages

After receiving and verifying all necessary user data and the message cipher key, the HBCI agent assembles a complete HBCI message, sends it to the HBCI server and waits for the server’s response. However, the HBCI agent cannot decipher the corresponding server's response message, because the message cipher key is not known, i.e. encrypted. Since this cipher key can only be retrieved by the mobile client by using its private key, the agent parses the server's response, extracts the ciphered cipher key (included in the encryption header segment HKVSK), signs and sends it to the client (**Fig. 7**).

4.2.5. Transport of HBCI Message Cipher Key to Client

As already mentioned, the ciphered HBCI message cipher key is transported from the agent to the mobile client, which in turn verifies the agent's signature and deciphers the message cipher key with the client's private key. The plain HBCI message cipher key is returned to the HBCI agent by using the procedure illustrated in **Fig. 5**.

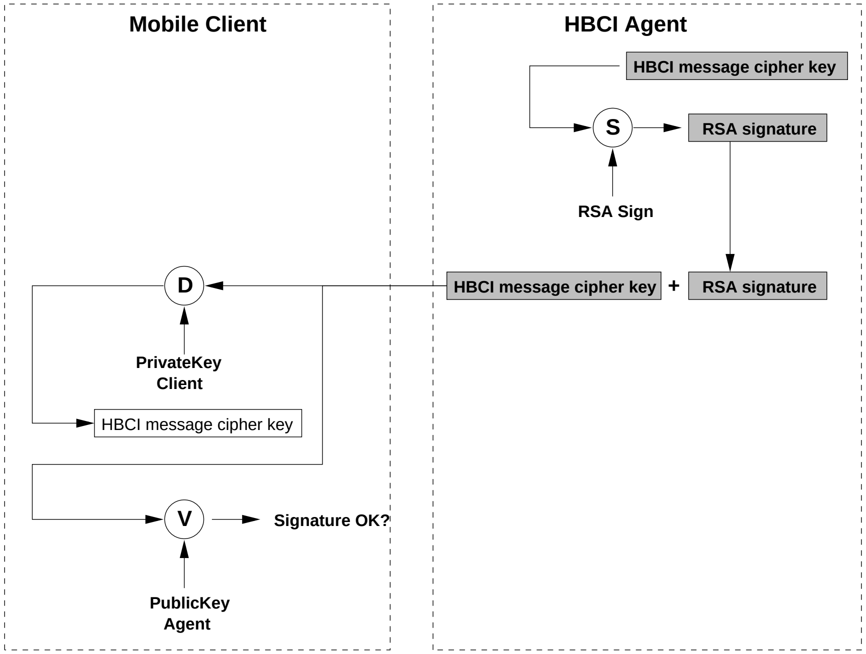

Fig. 7 Message cipher key decryption at client

5. Performance Evaluation

The Mobile HBCI concept is based on the necessity to allow specific (time-intensive) HBCI transaction procedures to be carried out on a powerful and high capable computer system outside of a mobile client (device). However, in order to guarantee the transaction security further, some security-related procedures, such as signing procedures, still have to be performed on mobile clients, e.g., cellular phones. In the following sections, the simulation system that was used to investigate the performance of Mobile HBCI is described and the assumptions made for the simulation are mentioned. An example scenario of an HBCI transaction that was used in the simulation, is described afterwards. Finally, the simulation results regarding the Mobile HBCI system time behavior are presented.

5.1. Mobile HBCI Simulation System

An SDL[11] simulation system representing the Mobile HBCI system is developed by means of the Telelogic's SDT[12] software. As shown in **Fig. 8**, the system consists of four SDL blocks which represent a mobile device, a WAP gateway, an HBCI agent and an HBCI server. The WAP protocols have not been implemented in the mobile client and WAP gateway yet. Hence, the WAP gateway is currently responsible only to forward the protocol data units (PDU) coming from the mobile device (client) to the HBCI agent (and vice versa). Moreover, the HBCI server is currently implemented only as a receiver and sender of HBCI messages without any further processing logic. The performance data is based on real measurements with an operating HBCI server of a German bank. Hence, the independent measurements data was used as pre-defined performance data of the HBCI server within the simulation system. In the following, the processes that are implemented within the SDL blocks *blMobileDevice* and *blHBCIAgent* are described.

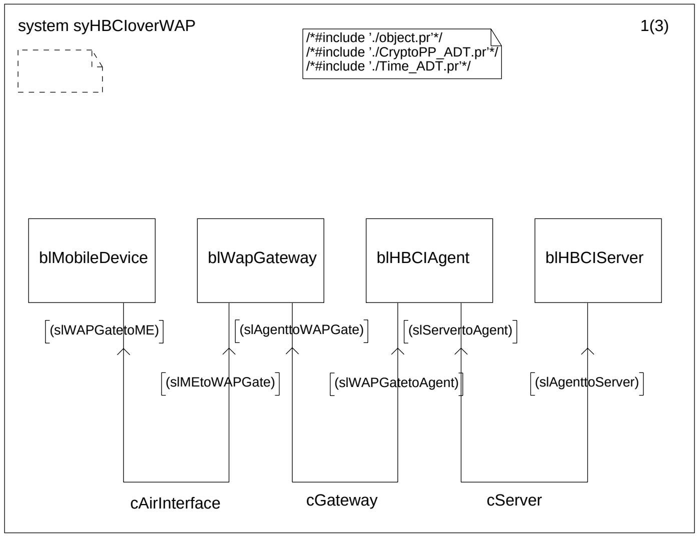

Fig. 8 The SDL simulation system of Mobile HBCI

[11] Specification and Description Language
[12] SDL Development Tool

As depicted in **Fig. 9**, the block *blMobileDevice* comprises four processes that have a significant impact on the system runtime. The load generator process *prLoadGenerator* generates the user data[13], sends it to the HBCI process *prHBCI*, and receives the transaction result later. The elapsed time between sending of the signal *sGVOReq* (initiate transaction) and receiving of the signal *sGVOResp* (transaction result) is defined as the total simulation runtime, i.e., the Mobile HBCI session time. The HBCI process *prHBCI* is responsible to initiate session initialization and termination. It sends the necessary information, such as user/transaction data, session identifier, or message cipher keys, to the HBCI agent. The process *prWIM* represents the tamper-resistant security module WIM[14] that is to be integrated in each WAP-enabled mobile device. It contains cryptographic functions for calculating hash values, signing and encrypting/decrypting messages, and verifying digital signatures of received messages. These cryptographic functions are implemented using the free C++ class library Crypto++ 3.2[15]. The performance of the cryptographic algorithms on the used machine (SUN Microsystems Enterprise server) is comparable with the performance of a special cryptographic processor, e.g., the Infineon's SLE66CX320P chip at 5 MHz clock rate. The process *prWAP* provides the interface to the WAP protocol stack. Since the WAP protocol stack is not implemented yet, the calculation of the transmission time on the air/radio interface only takes the additional protocol data overheads (caused by WAP) into account. Moreover, real measurements regarding the connection set-up time of a regular WAP data connection via a German GSM network were carried out separately and the obtained data was used within the simulation system.

The process *prDispatcher* that is contained in the block *blHBCIAgent* controls the communication path between HBCI agent, mobile device (client) and HBCI server (**Fig. 10**). The process *prGVOLogic* comprises the HBCI transaction processing logic[16]. The process *prSBox* represents the security module of the HBCI agent and is therefore similarly implemented like the process *prWIM* of the mobile device.

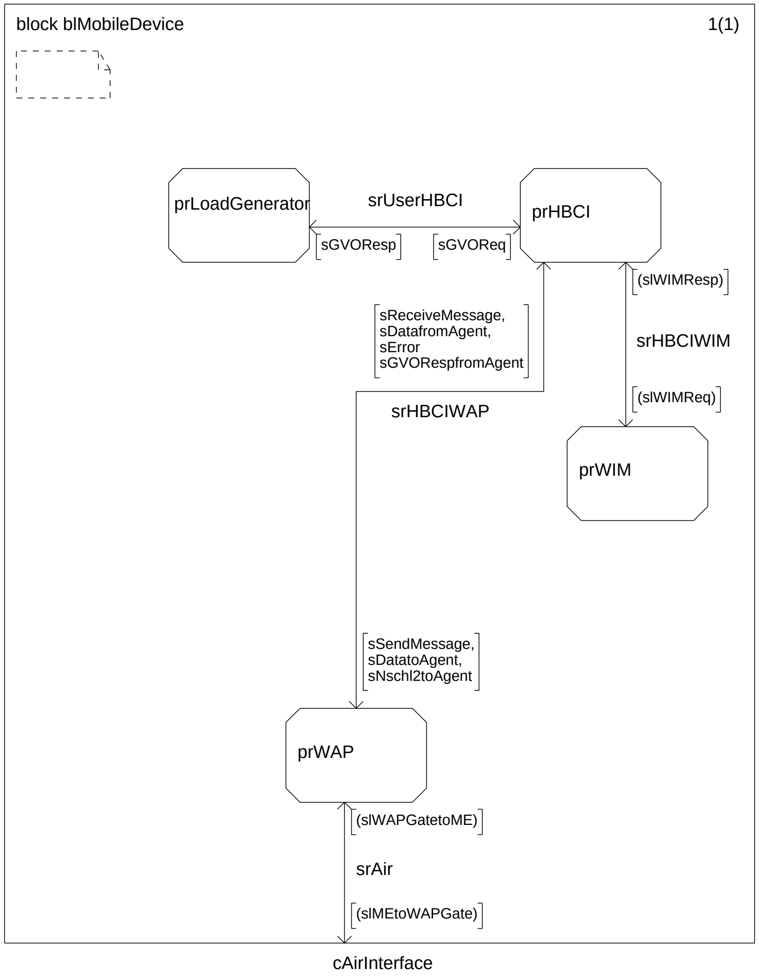

Fig. 9 The SDL block for the mobile device (*blMobileDevice*)

5.2. Example Scenario: Portfolio Order

An example scenario of a portfolio order (securities) transaction was used for the system performance evaluation. Before the HBCI transaction is initiated by the mobile client system, some transaction specific data would have to be

[13] see section 5.2
[14] WAP Identity Module
[15] available under http://www.eskimo.com/~weidai/cryptlib.html
[16] Here only the transaction logic for portfolio order (section 5.2) is implemented. Other business transactions can be added.

entered by the user manually. Then, the client system generates the corresponding HBCI data fields:

1. *HKWPO*: business transaction segment identifier (here: portfolio order)
2. *XFRA*: stock exchange center (here: XETRA Frankfurt)
3. *65,11EUR*: price limit and currency (here: 65.11 Euro)
4. *BUYI*: indicator for "buy" or "sell" (here: buy)
5. *LMTOGDAY*: type of limit and validity (here: valid for today)
6. *UNIT/200,*: number of units or nominal amount (here: 200 units)
7. *DE/870737*: identifier of the financial instrument (here: the securities reference)

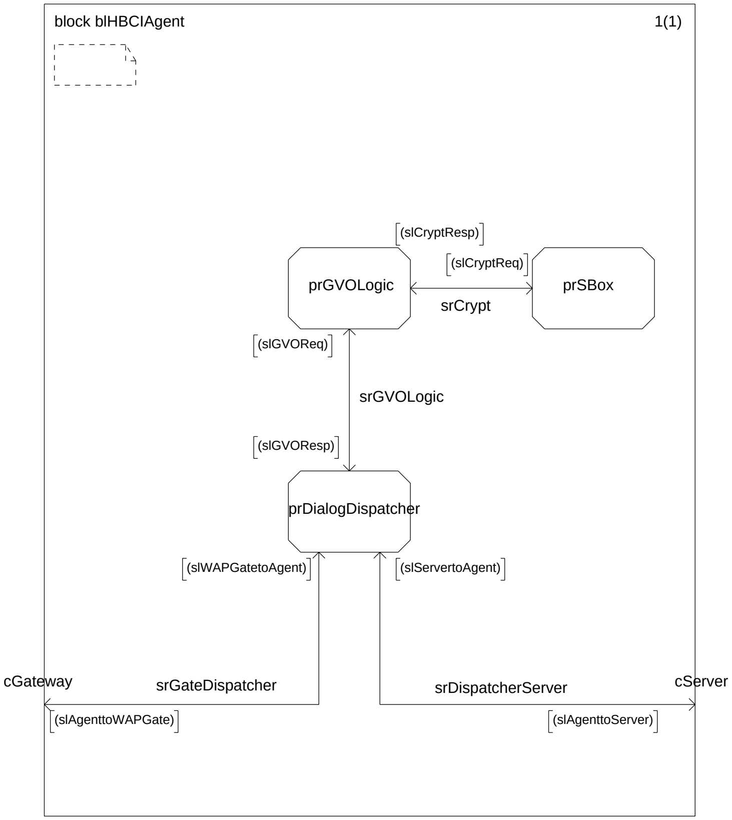

Fig. 10 The SDL block for the HBCI agent (*blHBCIAgent*)

Each data field is separated with a semicolon and assembled into the following HBCI data segment:

```
HKWPO;XFRA;65,11EUR;BUYI;LMTOGDAY;UNIT/200,;DE/870737
```

Then, the client system starts the procedure to initialize a new HBCI session and to process the corresponding transaction by communicating with the HBCI agent through the cellular system and WAP server, as described in section 4.2. The amount of each HBCI data segment being interchanged between mobile client and HBCI agent within the simulated security paper transaction from the initialization until the termination of the HBCI session is listed in **Tab. 1**.

DATA	C → A IN BYTES	A → C IN BYTES
Session initialization	1859	-
Response to session initialization	-	1398
User data + Session-ID	1152	-
User data + HBCI hash value	-	1232
Signature	2144	-
Message cipher key	1072	-
Ciphered message cipher key	-	1024
Deciphered message cipher key	1072	-
Response to HKWPO (portfolio order)	-	1136
Session termination	1924	-

Tab. 1 Messages exchanged between client and HBCI agent within a single Mobile HBCI session (portfolio order)

5.3. Results

Based on the simulations and measurements, the duration of each procedure within a complete Mobile HBCI session is ascertained as follows:

- WAP connection set-up time (measured): 15 seconds
- Session initialization (simulated): 14 seconds
- Processing times of the portfolio order at client and agent (simulated): 16 seconds
- Processing times at HBCI server (measured): 5 seconds

- Transmission delay on the radio channels with 9600 bit/s (calculated): 14 seconds

Hence, the total duration of a complete Mobile HBCI session (portfolio order) at a transmission rate of 9600 bit/s sums up to 64 seconds. **Fig. 11** shows the estimated session time (without WAP connection set-up time[17]) at different transmission rates on radio channel. For comparison, real measurements with a PC and an operating HBCI server of a German bank within a fixed network environment (wired Internet) have shown that an online HBCI transaction can be completed within 26.3 seconds on average. According to **Fig. 11**, it is obvious that the longer transaction time of Mobile HBCI is not mainly caused by the transmission delays on the radio interface, since the processing times at client and server systems already sum up to 37.4 seconds. This is particularly due to the fact that additional time-consuming procedures have to be carried out within a Mobile HBCI session to secure the data transmitted over the radio interface, i.e., between mobile client and HBCI agent.

To guess the market acceptance of Mobile HBCI, a rough calculation of the connection/online cost for one transaction would be helpful. In Germany, the current rate for online WAP-connection (via cellular GSM network) is about 0.20 € (Euro) per minute. Hence, a Mobile HBCI-based portfolio order transaction would cost about 0.23 €, which is relatively low, since usually the transaction cost (commission) for online-based orders is lower than for regular (offline) orders, e.g. orders by phone (operator-supported)[18]. In addition, by using Mobile HBCI, or m-banking service in general, the customer can access his/her account and make banking transactions anytime and anywhere.

6. Conclusion

A concept of a mobile banking system based on the German home-banking standard HBCI is presented. The concept provides a solution which combines the requirements on a secure financial transaction with the customer demands for user friendliness and cost effectiveness together. The existing home-banking standard HBCI is adapted to the typical situations the user usually finds within cellular systems, such as less powerful mobile devices, or more error-prone radio channels.

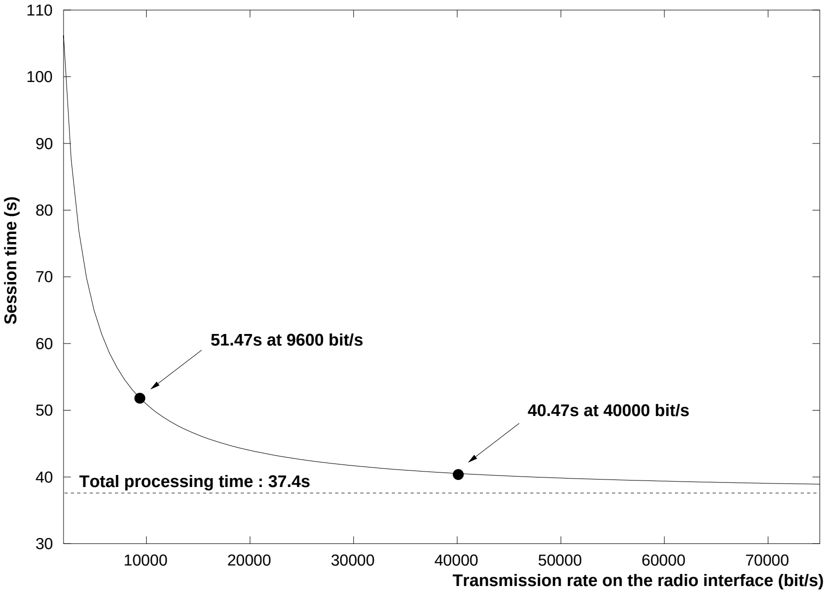

Fig. 11 Estimated Mobile HBCI session time

The performance evaluation study has shown that a single mobile banking transaction, e.g., portfolio order, can be completed within one minute, which can be further reduced when new cellular technology, such as GPRS[19], can be applied. By employing several cryptographic procedures that can be implemented as software or hardware on the server, and in future as hardware on mobile clients, e.g., as smart cards on cellular phones, the transaction security can be assured and thus accepted by all involved parties (customers, operators, banks).

Further works will focus on the extension of the current simulation system, such as implementing new types of business transaction like electronic wallet recharging, or specifying the WAP client and server functionality.

[17] In case of packet based data transmission, such as in GPRS, no WAP connection set-up is required.

[18] In Germany, the transaction cost (commission) for offline orders is usually twice as much as for online orders.

[19] General Packet Radio Service

7. References

[1] Bundesverband deutscher Banken (Association of German Banks), "HBCI – Home Banking Computer Interface 2.1 Specification", technical report, 1999.

[2] Ellsberger, J., D. Hogrefe and A. Sarma, "SDL – Formal Object-oriented Language for Communicating Systems", Hemel, Hempstead, Prentice Hall, 1997.

[3] Hußmann, H., "Secure HBCI-based financial transactions with mobile devices ", masters thesis (in German), Chair of Communication Networks, Aachen University of Technology, 2000.

[4] Müller-Veerse, F., "Mobile Commerce Report", technical report, Durlacher Research Ltd., http://www.durlacher.com, 1999.

[5] WAP Forum, "Wireless Application Protocol Architecture Specification", technical report, http://www.wapforum.com, 1998.