Financial Services for the Future - mobile, flexible, and agent-based

Jens Hartmann, Steffen Bretzke

Ericsson Eurolab Deutschland GmbH, Ericsson Allee 1, D-52134 Herzogenrath, Germany
E-mail: {Jens.Hartmann, Steffen.Bretzke}@eed.ericsson.se

Abstract

For some time, financial and commercial services over the Internet have gained remarkable and increasing attention. As this trend develops the range of services available to both businesses and individuals will grow. With the broader application field the need to provide simple but secure access to such services will get more and more momentum. Thereby access to the payment systems should be personalised and available to the users at all times and independent of network and terminal technology. The Flexible Financial Service (FFS) of the European ACTS research project CAMELEON will provide such a service building on the inherent autonomy of mobile agents.[1]

Keywords: *Agent Technology, CAMELEON, Mobile Agents, Voyager, Service on Demand, Homebanking, HBCI.*

1. Introduction

In computer science, the areas of Artificial Intelligence (AI), Distributed Systems and Object Orientation (OO) contributed to a new concept in distributed computing called Agent Technology. Currently, many computing scientists consider agents as a key to the issue of service provisioning for future telecommunications environments.

The traffic on fixed telecommunications networks has recently shown significant changes: the volume of data-based services is rapidly increasing and will soon exceed the volume of speech calls. This does not apply to mobile networks yet. However, even mobile networks are developing in this direction. Compared with the traditional networks mainly dedicated to phone calls, future networks need more flexibility to meet the new demands. Agents, especially mobile agents, seem to be better suited to provide the flexibility, because of their characteristics including autonomy, intelligence, mobility, coordination and cooperation.

In the future, network and service providers need to provide new, sophisticated services in a more direct and flexible way. Users can access these services anytime and anywhere, as long as their communication device can communicate with the network.

Using agents, services can be easily subscribed to download or migrate to the user terminal device. The user only needs to subscribe to a certain type of agent, which will provide the preferred “look and feel”. This new service-provisioning paradigm can be identified as “service on demand” and “look and feel on demand”.

Using agent-enabled systems, agents may represent almost any component of the system. Some existing application scenarios can be executed in a more effective and flexible way. E-commerce services, for instance, are traditionally transaction-based. With an agent-based approach, however, it would be easy to build these applications in an asynchronous way.

The work described in this paper has been undertaken in the framework of the *CAMELEON* project [CAM98]. The project developed and tested service roaming applying Agent Technology to a mobile network environment using the Virtual Home Environment (VHE) as a test case.

(1) This work was partly supported by the Commission of the European Community (CEC) as part of the ACTS CAMELEON project (AC341)

2. Service Description

The ever-growing demand for user mobility increases the need to conduct transactions such as electronic payment, ticketing, home banking, etc. anytime and anywhere. This leads to an effort to integrate existing electronic payment systems into the mobile environment. Mobile commerce is a subset of *Electronic Commerce* and deals with the electronic commerce issues in the mobile environment. Mobile commerce delivers significant opportunities to those working in the banking, transport, retail, and communication industries.

The Mobile environment comprises many wireless technologies, such as wireless LAN, GSM, wireless ATM, etc. These systems have their invidual characteristics that may impact on the realisation of mobile commerce. However, from the consumer's point of view, mobile commerce should meet the following requirements:

- Simplicity
- Response times comparable to traditional electronic transactions
- Security
- Convenience

The rapid development of electronic commerce presents great opportunities for network operators to introduce new services in conjunction with mobile commerce. Nevertheless, due to some limitations of mobile stations, such as small displays and low bandwidth, some modifications are necessary to integrate electronic commerce applications in the existing GSM system.

Financial services for mobile telecommunication networks cover a wide spectrum of business services. The two most important types are banking services and electronic payment. These services are briefly described in the following sections.

2.1 Homebanking Services

A bank offers banking services to their customers who may access these services either at their bank office or elsewhere over some computer. In this case, the customers need some additional, specific software usually distributed by their bank over the network (homebanking scenario).

Homebanking is an alternative way of selling bank products. It has existed for several years and is attracting more and more private customers. Homebanking provides access to bank products, information and advertisement anytime at home, in the office and while travelling. But at the moment, most customers need special software from their bank in order to access these business services. Homebanking would be much more convenient for both banks and clients, if telecommunications networks or service providers were able to offer financial services to their customers in a more flexible way.

Banking services cover the following important business cases:

- account operations (opening, etc.)
- balance inquiry
- sales statistics
- transfers (domestic and foreign)
- credit note / debit note (single and collective)
- loading of the stored value chip card
- financial reports
- credit card sales
- check orders
- stock price quotations
- currency exchange rates
- marketing and service offers of the credit institutes

2.2 Electronic Payment

Electronic payments with credit cards over open networks, such as the Internet, become common and part of our daily life. In a typical credit-card-based payment transaction, the customers enter their credit card number in a payment form available on the merchant's World-Wide-Web page, send their data off and wait for the purchased items to be shipped. The information that needs to be exchanged between the merchant and the customer include the credit card number, the expiration date, and sometimes also the customer's address. An intruder might eavesdrop into the insecure connection and intercept the credit card number for illegal use. To prevent this, a connection secured by the SSL (Secure Sockets Layer) protocol should be used, but unfortunately SSL only protects the data against network monitors and spying, it cannot prevent the merchant from misusing the customer's credit card information.

Secure Electronic Transaction™ (SET™) is a standard developed jointly by VISA and MasterCard

and is published as an open specification to the industry [SET97a]. SET™ is a complex protocol that uses advanced cryptography for securing credit card payment transactions over open networks. SET™ does not just provide the security of the sensitive information exchanged during a transaction, but guarantees the authentication of each party (cardholder, merchant, and acquirer) using digital signatures. With SET™, the payment card company gets involved in the middle of the transaction and acts as a middleman. SET™ could also accelerate the payment settlement process, since the financial institutions are involved up front. The transaction is secure, since the merchant will never see the cardholder's credit card information. Instead, that info goes to the financial institution, which verifies the card info and the amount. The involvement of the financial institution ensures that the merchant can determine directly if the cardholder's payment card is valid or not.

There is one point regarding the security that has been left out in the SET™ specification, namely the physical level of security: unfortunately, SET does not define how to store the cryptographic keys.

The next SET™ specification, version 2.0, is in progress and will handle these issues and propose the usage of smart cards to provide more security for the storage of secret keys. Some points will also be considered in the next SET™ version such as the independence of cryptographic algorithms, debit payments, etc.

With MasterCard and VISA putting their weight behind SET™, the standard should gain wide acceptance in the Electronic Commerce community and establish a solid basic credit card payment mechanism for open networks.

3. Requirements

The success of GSM, the second-generation mobile communication standard [Mou92], relies, among other things, on the possibility of roaming between networks – and thus between countries –using a single subscription. This implies that subscribers are reachable using a single number and receive a single bill from their home service provider. In fact, the three most important topics for future mobile users will be similar to those of current GSM users:

- Easy handling of the desired telecommunication services, including the opportunity to customise the 'look and feel' of services and obtain 'services on-demand'
- Global availability and consistent performance of telecommunication services
- Convenient billing with a single point of contact

However, the future telecommunications world will not be homogeneous, and therefore it will not be easy to reach these goals. The problem has been identified by ITU and ETSI, the telecommunications standardization bodies, which took measures to permit 'service roaming', also known as service portability. The VHE concept [Har98, VHE98] adopted this idea, enabling a visited network to obtain information about the user's Service Provider during the registration procedure and other information such as the user's personalised service profile and the identification of service capabilities needed for the execution of provider specific services. While various networks may realise a service in different ways, the VHE concept enables the user to access and use the service in the same way on any network. The VHE is being standardised in ETSI SMG 1 and ITU SG 2 for implementation in the Universal Mobile Telecommunications Network (UMTS) and the International Mobile Telecommunications 2000 (IMT-2000), the third-generation mobile networks [ITU98].

For these third-generation networks, most countries have allocated a frequency spectrum in the 2 GHz frequency band. The UMTS air interface will utilise W-CDMA for the wide area environment with a proposed TD/CDMA structure for the unpaired banks. In implementing this solution, the ETSI representatives follow the specification of UMTS aiming to support:

- low-cost terminals
- harmonisation with GSM
- FDD/TDD dual-mode operation terminals

3.1 Requirements from Network / Service Providers

The Internet community, the telecommunications market as a whole and the mobile telecommunications market in particular are experiencing an enormous growth. Mobile network operators and service providers know that the continuous growth leads to a

huge potential market for many commercial on-line services.

A number of secure transaction processing schemes have been proposed to allow ordering and payment activities over the Internet. However, up to now these schemes have not been evaluated when accessing the Internet over the air link.

Since mobile communications are still quite expensive, the bandwidth is limited and bit errors occur frequently, it is essential to investigate dedicated solutions for mobile electronic commerce services.

Thus, the main requirements for financial services coming from the network and service provider perspective are:

- secure transmission of the financial data
- data integrity
- limited amount of data
- scalability
- rapid, easy and economic creation, testing and introduction of the service
- Services should not crucially affect the existing network infrastructure

3.2 User Interaction Requirements

Most modern applications communicate with their end users through a graphical user interface (GUI). The main purpose of the GUI is to hide the high complexity and abstraction of software through a user-friendly interface, so that subscribers do not need to spend a lot of time and energy to study and understand the internal functionality and logic, before they can use the application. The GUI determines the users' impression of an application, and has an important position in an application. The general requirements for GUI design are as following:

- the interface is easy to understand and use
- the style has a clear and consistent design
- the look and feel is almost identical and customizable for all terminals, displays and services
- all end-terminals are Java and Mobile Agent capable
- the help information is well-documented and easy to access

3.3 Support of Roaming Users

One of the most important features of the VHE concept [VHE98] is the operator- and location-independent support of a customized user environment, offering roaming users an identical look and feel for user profiles and services. The VHE concept sees the entire network as interconnected sub-networks. Each user in a sub-network has the same authority policy and a sub-network can be defined as a *region* according to the Mobile Agent System Interoperability Facility (MASIF). A region consists of a number of *places*, which are agent execution environments. The places in a region can belong to different agent systems (e.g. vendors). All users have their own ids and preferences stored in user profiles in their home region. The user profiles are accessible from anywhere in the network.

If the user profiles are not stored in the region where the users are present, the users may be identified as roaming users. When roaming users try to register in a region, the user agent on the terminal loads their user profiles from their home regions. As an alternative, the user agent may register users by loading the user profile directly from a local storage medium, such as a hard disk or a SIM-card.

After registration, users have access to the services defined in their user profiles. If a service is not available in a region, a copy of the service provider object may migrate to this region, in order to reduce the traffic volume between the network nodes and to improve the performance. For a lot of services provided by third-party service providers, the migration of such services is limited due to security reasons. So other concepts are wanted.

The user profiles should contain configurations for all subscribed services, so that services can be directly used without creating a connection, if the GUI part of the service is already downloaded. This approach may reduce the load on the network resources and lead to a system that scales more easily when the network load increases.

3.4 Agent Platform 2000

The ***CAMELEON*** consortium has selected the Voyager agent platform of ObjectSpace [Obj98] as the Agent Platform 2000 described in the Technical Annex of the project [CAM98]. Several performance tests have shown that Voyager has the best results in agent and data transmission, system boundaries and message exchange [Son98].

Agents in the context of the ***CAMELEON*** project are considered to be a combination of the static and mobile agents described above. In this definition, agents can interact by exchanging messages using a universal language, and, when appropriate, halt execution, migrate to a different network location and continue execution. Potentially, agents executing in a device (e.g. a mobile phone) may roam in networks creating the impression of migration. Such agents can still be considered as static entities as they continue to execute in the same host device, but as the device roams between networks, the agents executing in the device become addressable on different networks.

4.1 Basics of FFS

FFS allows telecommunications users to make financial business transactions offered by their service provider. FFS is part of a Virtual Home Environment (VHE), the concept developed for UMTS and standardized by ETSI [VHE98]. VHE includes the support of service mobility (also known as service roaming). In such an environment, users access their customized environments and services independent of the underlying network.

Today, for example, most homebanking services require bank-specific software covering all services the bank provides over the network. Consequently, the users may have various software packages installed on different computers, which they need to maintain. Moreover, the users do not have an identical 'look and feel' of the service, because of the user profiles and configurations are stored separately on each machine. Integrating the FFS directly in a telecommunications network could change this situation, because an FFS application server acts as a universal bridge interface between users and banks, see Figure 1. All users have their own user profiles and a consistent 'look and feel', independent of bank and network.

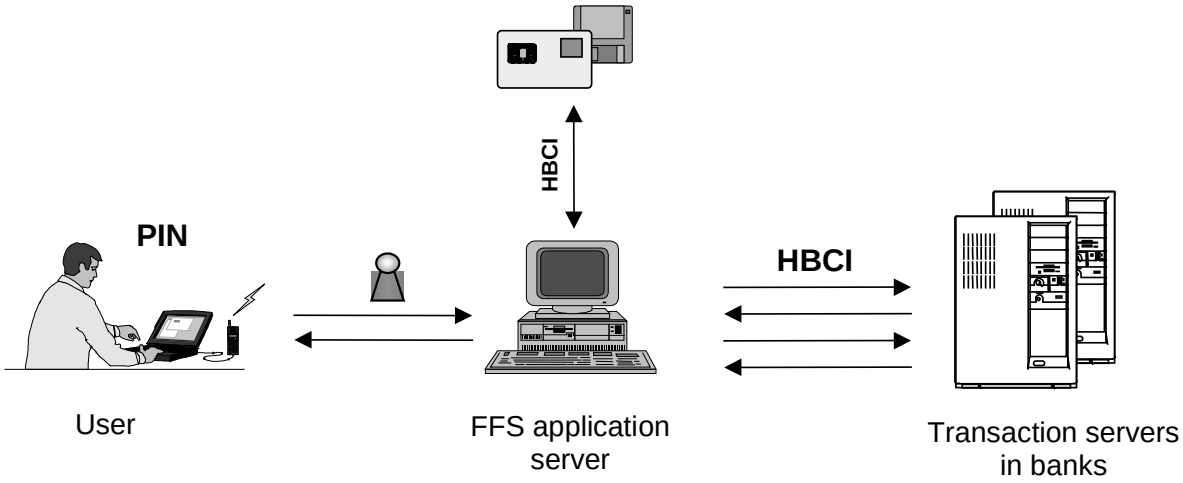


Figure 1: The FFS service scenario

4. Flexible Financial Services

The FFS architecture contains a service provisioning system on top of the existing telecommunication environments. Similar to other prototypes in the CAMELEON project [CAM98], the FFS uses the agent platform 2000 applying current technologies to new services in order to show the feasibility of implementing a Virtual Home Environment with mobile agent technology.

Based on this architecture, our team evaluated a number of agent platforms. The team decided to choose Voyager from ObjectSpace [Obj98] as the basic development platform, because Voyager is the platform offering the most extensive functionality, the best performance, and very high compatibility to CORBA.

4.1.1 FFS Homebanking

Figure 1 shows the FFS homebanking scenario; the transaction servers, waiting to process transaction requests for their clients, are operating in the domain

of a bank. An FFS homebanking server is running in the intermediate network. On one hand, this server acts as a homebanking service provider for the users in the FFS system, on the other hand as a homebanking client from the view of the transaction servers in bank system. The transaction specific user data are stored or accessible at the server position. The homebanking server communicates with the transaction servers and the secure mediums over a common financial protocol (in this case HBCI).

A user can download a FFS homebanking client, which can be implemented as an FFS terminal agent to access financial services. This client can be customized before and after the downloading. After starting the client, the user can create homebanking agents, give them tasks and launch them. The agents will travel to the homebanking server, process the tasks and return results. Every transaction should be protected by a unique pin code.

4.1.2 FFS Electronic Payment

Similar to the homebanking application, there are a variety of electronic payment systems for purchasing items online. Some of the most popular payment systems are SET™ [SET97a], eCash [ECP98], Cybercash [CCP98] and SmartCard systems. SET™ is a Credit-Card-based payment mechanism, while the rest are primarily prepaid electronic cash systems. SET™ is used for medium and high value purchases while the other mechanisms are preferred for small change transactions. Offering a common payment mechanism and interface greatly simplifies the user experience with the payment services. The standard SET™ architecture is illustrated in Figure 2.

The SET™ architecture is designed to protect the financial information involved in a payment transaction between a cardholder, merchant and acquirer. The architecture does not impose requirements on the transmission of the transaction's order information during the shopping phase. A SET™ payment transaction involves several parties:

- **Cardholder**, an authorized holder of a payment card supported by an issuer, and registered to perform electronic commerce.
- **Merchant**, providing goods, services, and/or information, accepting electronic payments.
- **Issuer**, a financial institution that supports issuing payment card products
- **Acquirer**, a financial institution that supports merchants by providing services for processing payment card transactions.
- **Payment Gateway**, a system that provides electronic commerce services to the merchant in support of the acquirer, and interfaces to the acquirer to support the authorisation and capture of transactions.
- **Brand**, a franchiser of payment systems/instruments.
- **Certificate Authority (CA)**, an agent of one or more payment card brands that provides for the creation and distribution of electronic certificates for cardholders, merchants and payment gateways.
- **Banking network**, the existing private network operated by a payment card

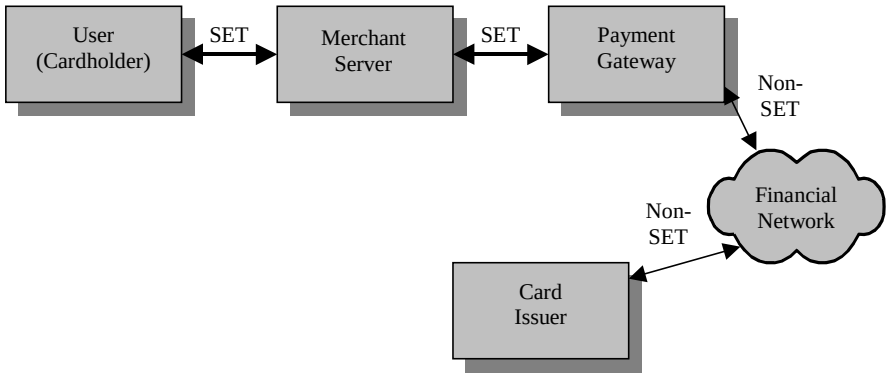
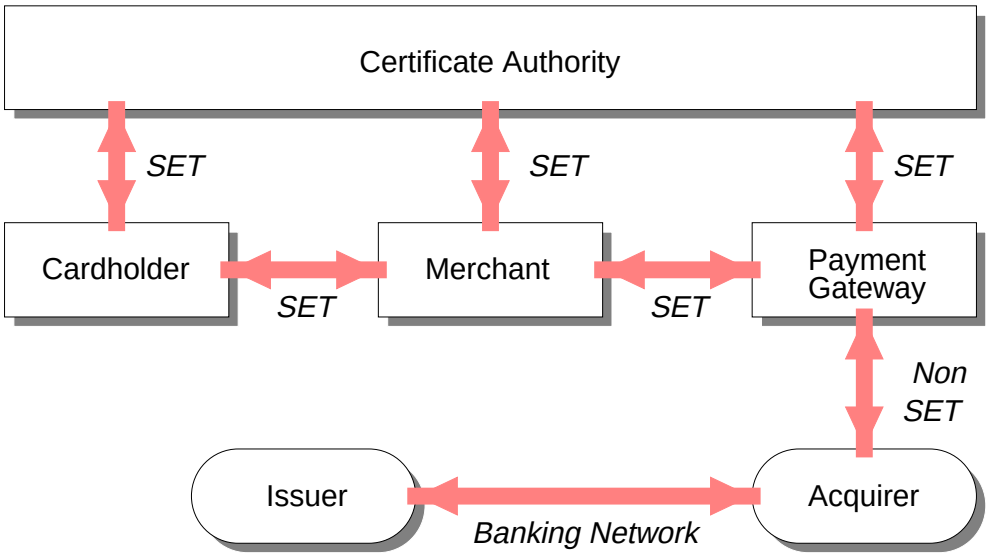


Figure 2: Standard SET™ architecture

brand that links acquirers and issuers of payment cards.

Figure 3 shows the major roles in the SET™ process and their interaction.



In the VHE environment, it is the role of the payment service providers to, don't be surprised, provide payment services. Such a modified SET™ payment architecture is also used in the ACTS OnTheMove mobile middleware architecture [OTM98]. The modified SET™ architecture for Cameleon FFS payment service is shown in Figure 4.

Finally, Figure 5 shows the FFS electronic payment scenario where the electronic shops host the Merchant servers that process the order requests from their clients. An FFS Electronic Payment server is running in the intermediate network. This server acts as a payment server for the users in the FFS system. The user specific keys and certificates are stored or accessible at the Payment server. The Electronic Payment server communicates with the Merchant server over a common payment protocol such as SET™, eCash or Cybercash.

The FFS electronic payment client is downloaded to the user's terminal that can be implemented as an FFS terminal agent accessing financial payment services. This client can be customized before and after the downloading. The user creates ePayment agents, gives them tasks and launches them. The agents travel to the electronic Payment server, process the tasks and return the results. Every payment/order must be protected by proper security mechanism such as a PIN.

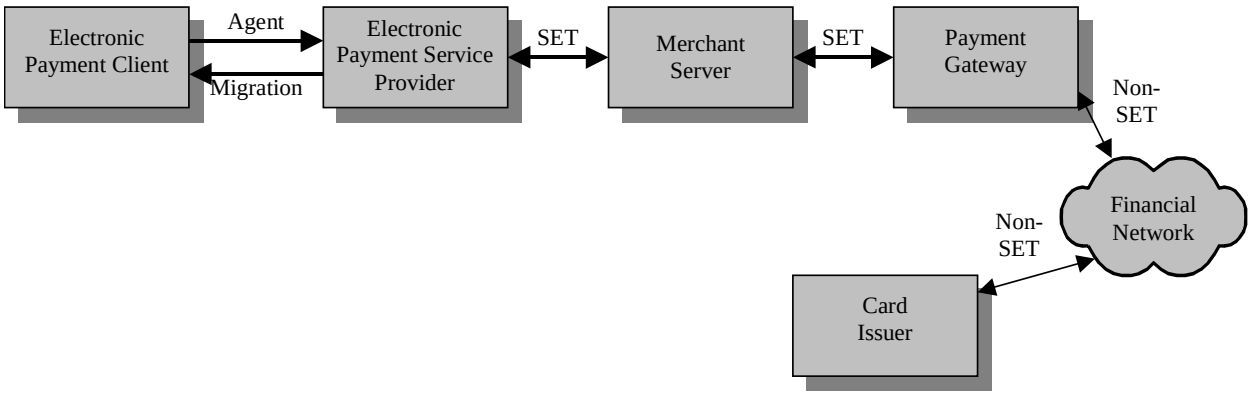


Figure 4: CAMELEON SET™ architecture

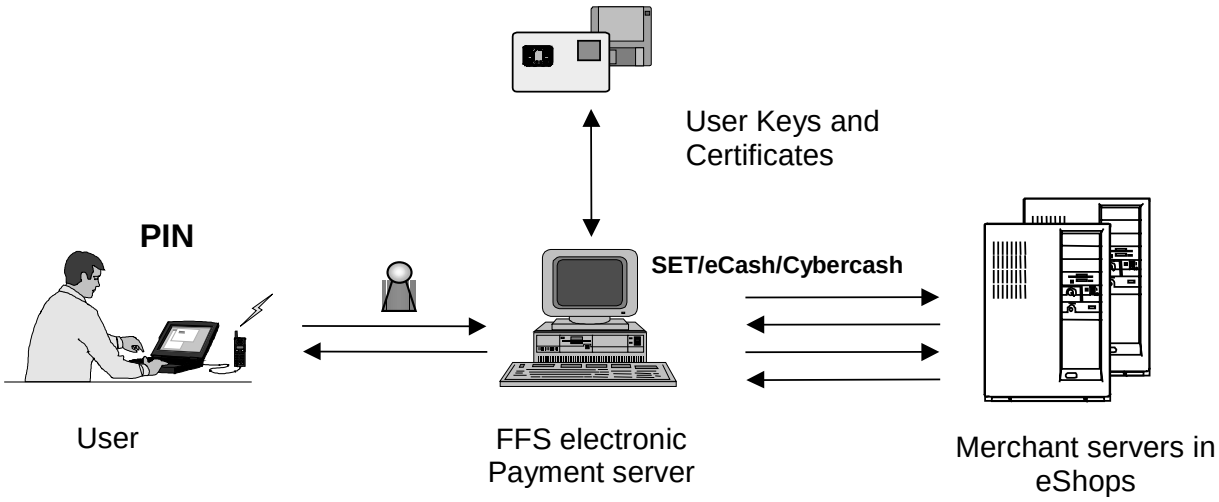


Figure 5: FFS Electronic Payment scenario

5. Conclusion

In the framework of the research project *CAMELEON*, which is funded by the European Commission, we have implemented an agent-based homebanking service in the commercial mobile agent platform Voyager from ObjectSpace. This service, which has been introduced briefly, allows triggering a huge set of banking transaction over the air-link with the help of mobile agents. The main processing of the service is undertaken locally at a bridging homebanking server, which performs the protocol specific communication with bank server based on a new German banking standard called HBCI. A mobile user can access the homebanking service by simply downloading and starting a Homebanking Terminal Agent using his Terminal Agent, sitting on top of the Java-based Voyager platform on any system with a JAVA Virtual Machine.

This homebanking service shows how to use agents for enhanced service provisioning. It proves that it is reasonable to apply Agent Technology in future telecommunication networks for end-user services. In particular, the service solves two important challenges for future mobile networks with the help of Agent Technology, namely the customisation of the 'look and feel' of services and the download of 'services on-demand'. In the near future it should also be investigated, if agents also bring some benefits for to telecommunication network and management services.

6. References

[CAM98] CAMELEON Consortium. An Open Communication Environment Using Agent Technologies, ACTS 341; Technical Annex Part B, March 1998.

[HBC97] Bundesverband deutscher Banken. *HBCI – Schnittstellenspezifikation*. Version 2.0 (in German), July 1997.

[ITU98] International Telecommunication Union. *IMT-2000*. http://www.itu.int/imt/

[Jav98] Sun Microsystems. *JAVA*. http://java.sun.com/

[Kel98] Keller R., Zavagli G., Hartmann J., Williams F. *Mobile Electronic Commerce: GeldKarte Loading Functionality in Wireless Wallets.* International IFIP/GI Working Conference: Trends in Electronic Commerce, Hamburg, June 1998.

[Mag96] Magedanz T., Popescu-Zeletin R. *Towards "Intelligence on Demand" - On the Impacts of Intelligent Agents on IN.* 4th International Conference on Intelligence in Networks, Bordeaux, France, November 1996.

[Mou92] Mouly M., Pautet M.-B. *The GSM System for Mobile Communtns.* Pu by authors, 1992.

[Obj97] ObjectSpace. *Voyager Core Technology User Guide.* Version 2.0 Beta 1, 1999

[VHE98] ETSI TR 22.70 Universal Mobile Telecommunications System (UMTS); Service aspects; Virtual Home Environment (VHE). Version 3.0.0 . March 1998.