The *ProCard* mobile banking system

Traian SURCEL, Felician ALECU
Academy of Economic Studies, Bucharest

The mobile banking involves the use of some mobile telecommunication devices (such phones or PDAs – Personal Digital Assistants) in order to complete, in a secure manner, banking transactions (like payments, transfers, account information and so on). It doesn't matter where the user is physically located. Also, the hour when the services are requested is not important anymore, because, thanks to the internet banking, the offices are virtually opened 24 hours per day.

The ProCard system represents a suite of applications used to perform mobile banking. It was intended to be a universal solution that allows EFT, Internet and mobile banking in a single package. No special software or hardware is required.

Keywords: *Internet banking, mobile banking, electronic transactions, electronic funds transfer, mobile terminal, PDA, SSL, parallel processing, grid networks, clusters of workstations, grid processing..*

Electronic payments and mobile banking
Today the modern society is encouraging the shift from the traditional methods of payment (like cash, bank transfer and so on) to the electronic ones (e-payment, mobile banking, EFT). The most popular payment methods available for the customers from our days are described below:

a) traditional methods – like cash in advance, cash on delivery, bank transfers and payments – can be used to pay for goods purchased from classical stores or from e-commerce websites by orders placed over the Internet. In this last case, the payment and delivery are made in the conventional way, only the order is placed using the Internet;

b) electronic methods – involve e-payment, e-banking, mobile banking, electronic funds transfer, e-check, e-cash, smartcards and so on. The transactions are completed in a secure manner by using the encryption.

Basically, an electronic payment system involves the use of a digital financial instrument that allows the money exchange between the buyer and the seller. The most common issue regarding the electronic payments is the transaction security.

The most important barriers in developing the electronic payment systems are the following:

- incomplete legal infrastructures regarding the card transactions and the lack of a framework involving the fraud by using stolen or lost credit cards;
- underdevelopment of the credit card industry in some countries;
- the existence of the explicit consent – a transaction cannot be considered as being valid until the owner of the credit card is physically signing on a specific receipt;
- the cash payments are preserving the anonymity, while the electronic payment systems not.

The major players of a successful e-commerce business are the following:

- seller – it should have a website with specific capabilities and an Intranet network to be used to quickly process the orders;
- customers – consumers having Internet access and owning credit cards to be used for payments. These customers should accept the idea of buying an item by seeing its pictures and reading about its features but without actually inspecting it;
- transaction partners – financial institutions that are able to process electronic funds transfers and the credit card payments;
- international express, overland transport and air freight companies – are moving physical items form the seller to the buyer;
- authentication authorities – they guarantee the security and the integrity of the transactions;
- government – it provides the legal framework for the e-commerce activities and also it protects the customers from fraud;
- Internet connection – reliable infrastructure

and access packages not based on the time spent or on the traffic performed.

The *ProCard* application is a mobile system designed and created to process the electronic funds transfer transactions. The system is able to support Internet and mobile operations generated by using classical or mobile devices.

For the *Internet banking*, a customer needs an Internet connection, no matter if this connection is a classical one or mobile. For the *mobile banking*, an Internet connected PDA with magnetic card reader should be used. Any card transaction is initiated using the client browser.

The very quick development of the mobile devices allows the banking transactions to be performed through mobile phones and *PDA*s. This is called *mobile banking* and implies the existence of some dedicated services.

Security of banking transactions performed over the Internet becomes a huge potential problem. A very good method that can be used to protect a private network is the implementation of a firewall between Internet and Intranet. This firewall will filter the packets that transit the network according with the security policy defined at the system level.

The *SSL* protocol allows verifying the identity of a *WEB* server based on a digital certificate issued by a certification authority. Secure data transport over the Internet is done by using encryption methods.

Today, the mobile banking is based on dedicated services offered by the telecommunication operators. Some systems are using *SMS* messages exchange but others involve smartcards that store the details of the accounts that are used. The security of these transactions is one of the most complicated challenges that need to be addressed.

The service can be requested anytime by a user located anywhere. Customers do not need to go to the bank office and also there is no need to access a computer having an Internet connection in order to perform the banking transactions.

Other applications of mobile banking are connected with different financial services like online brokers, online banks, wealth managers, stock trading and so on.

Of course, the mobile banking has some limitations. Customers cannot access accounts that are not assigned with their smartcards and they cannot pay at the supermarket by using the phone, for example.

The number of user accessing the mobile banking is growing faster from one year to another. The use of the *3G* mobile networks will generate the development of more sophisticated services involving multimedia.

In the last years, the banks invested o lot of money to develop Internet banking systems. Now, they need to adapt to the market and to offer to the users mobile banking solutions in the shortest possible time.

The ProCard system

ProCard is intended to be a universal solution that implements electronic funds transfer (also known as *EFT*), no matter if the customer is using a mobile or a wired Internet connection. In order to use the application in mobile mode, it is enough to use a *PDA* (Personal Digital Assistant) having Internet access. The Internet banking approach involves only an Internet connection.

The future of mobile banking will be represented by such applications that support mobile, Internet banking and *EFT* (Electronic Funds Transfer) transactions in a single user interface. In such a way, the mobile banking will be able to cover all the types of applications demanded at the market level.

Today, the *EFT* transactions are basically performed by using a dedicated device that is able to read a bank card. The user enters the PIN code by using a secured *PINPAD*. The *EFT* terminals are permanently connected to the bank by using dedicated wired phone lines.

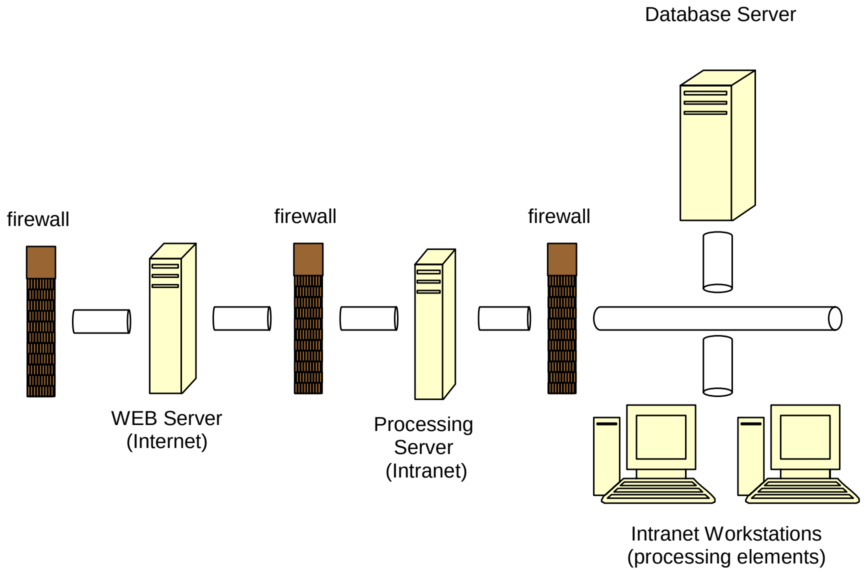
By creating applications that are able to join online banking with *EFT* ones, the mobile banking will become very attractive for big retailers (like hypermarkets and supermarkets) because they will not need to invest so much money in the infrastructure (wires, cables, dedicated lines and so on). The customers will be able to pay by the credit cards using mobile devices (*PDAs*) located at the payment points and connected with a dedicated bank server by using the Internet.

All the requests by this type will be processed by specialized bank servers. If the expansion of the mobile banking will grow faster, the banks will have huge problems in processing the incoming requests generated by the mobile systems. The dedicated servers will need to complete very fast a huge number of the transactions but in a secure manner. In order to achieve very good response times, the servers could dispatch the transactions in the bank Intranet by implementing a grid network of workstations.

The card transactions should be processed as fast as possible. To achieve such an objective, the system is actually processing the transactions is a parallel manner by using a grid network. The use of a grid network is an economical and convenient solution because it is based on existing resources (computers located in the Intranet of the bank) that are not 100% used during the day. Their idle times could be used to process bank transactions generated by the mobile devices. Once a transaction is processed by a workstation, an answer is sent back to the server and the mobile device will receive a message containing the result of the transaction processing. Also, the parallel processing of the transactions will guarantee very quick and accurate responses even if the number of concurrent requests has a very large value.

Today, the *EFT* transactions are completed by using dedicated phone lines. A special device is calling the bank server and is discussing with it by using a predefined protocol. The average time of a transaction is around 5 seconds. The maximum number of workstations that can be connected to the *ProCard* system is equal with 32.000. If a number of 32.000 of card transactions are generated in the same time, the *ProCard* system, when running at its full capacity, is able to complete all the requests in 5 seconds. A classical system will need 160.000 seconds to finish (45 hour, almost 2 days). The parallel processing of the card transactions generates a huge speedup at the application level.

The resources required by the application are presented in the next picture.



The resources required by the *ProCard* application

The components of the *ProCard* system are listed below:

1. *The application at the WEB server level* – written in *ASP* (*Active Server Pages*), it represents the interface used by the customer in order to specify the transaction details into the browser. This application also includes an administration module that can be accessed by providing a special password;

2. *Processing server* – this application is written in *Visual Basic .NET*. It receives the transaction details from the *WEB* server and places

all the requests into a waiting queue. The scheduler manages the queuing system and it implements the system serving discipline based on priorities.

3. *Processing clients* – are applications running on the workstations and, speaking in terms of queuing theory, they represent the service facility units. These clients are processing the card transactions coming from Internet and the results are sent back to the server and finally to the browser. More than one client is allowed to run on each workstation.

4. *Database application* – allows performing queries and updates in a graphical form focused on the non-initiated users.

Conclusions

Grid networks represent a distinctive and very modern field of the parallel and distributed processing. Excluding some limitations, the grid processing offers huge opportunities to exploit the parallelism. For this reason, in the last years a lot of applications of waiting queues in grid processing were developed. The parallel processing of bank transactions done by using credit cards is performed with the help of a grid network. The complete implementation of *Internet* and *Mobile Banking* allows to the individual users to access the *Pro-Card* system. Another possibility is to connect a few systems together in a transactional network that will cause faster response times and better characteristics. I can conclude that grid processing can definitively contribute to the expansion of the mobile banking.

References

[1] Tanenbaum A. S., *Computer Networks*, Prentice Hall, 1996

[2] Surcel T., Mârşanu R., Pocatilu P., Reveiu A., Bologa R., Alecu F., *WEB Technologies and Databases*, Tribuna Economică, 2005

[3] Brewer M., Internet Banking: Strategies, Tools, and Best Practices, Sheshunoff & Co, 2000

[4] Chapman G., Internet Banking and Shopping, Bernard Babani Publishing, 2004

[5] Noonan W., Dubrawsky I., *Firewall Fundamentals*, Cisco Press, 2006

[6] Cheswick R., Bellovin S., Firewalls and Internet Security, Addison-Wesley Professional, 2004