

An Approach to A National E-Payment Architecture

Süleyman Kondakci, IT Consortium of Turkey,
Division of Information Security, The Netsekuritas
kondakci@itconsortium.org

Abstract- With the increasing deployment of Web-enabled technologies, electronic fund transactions and home banking is rapidly taking place over the Internet. There is a growing need for a solid and robust electronic business and payment system. The current payment system bears several types of difficulties for Internet users. Financial institutions, banks, customers and merchants, around the country, are willing to take the advantage of a failsafe and efficient electronic payment and transaction system with a hierarchical payflow structure. The hierarchical structure will mainly comprise autonomous regions. The major requirement for the autonomous regional system should, at a minimum, provide interoperability among national and international systems and products. This paper, will, in addition to a proposed national e-payment backbone, pinpoint technology conformance to international standards. Most individuals that use home banking use telephone based services, which have been in use for several decades. These systems are both difficult to use and bear some major security threats. This situation is expected to change over time with the aid of the rapidly evolving Web-enabled services.

Keywords: Common e-payment structure, home banking, digital fund transfer methods, Web-enabled transaction.

I INTRODUCTION

This paper provides the technical overview of a proposed Banks Internet Payment Center (BIPC), which has mainly been prototyped in streamlining the payflow processes from trader-to-bank and bank-to-bank transactions taking place over the Internet. BIPC is designed, in accordance to the FIX protocol [1] recommendations, to serve the e-business with:

- The basis for building national e-payment standards and technical models that comply with the *European ePayment System*, derive open trading requirements in parallel with *IETF's Internet Open Trading Protocol* and the *FIX Protocol*.
- A means to reduce the clutter of unnecessary telephone calls and scraps of paper, and facilitate targeting high quality information to specific institutions, banks, and other e-payment participants, and individuals.
- An open standard that leverages the development effort of Web-enabled services so that technologies can efficiently create links with a wide range of counter-parties.
- Ready access to the industry, with the indispensable reduction in marketing effort and increased potential client base.
- Reduced security risk figure, increased Internet throughput, and faster e-payment flow processes.

II CURRENT SITUATION

Enterprise banking uses home-brewed payment system based on dedicated payflow structure between the enterprise and the financial institution. These systems are both difficult to use and bear some major security threats. Most individuals that use home banking use telephone based services, which have been in use for several decades. However, recently, the majority of banks have established their own Internet

banking services independent from others. Head quarters of the banks have deployed the necessary processing centers, where their branch offices carry transactions through the head quarters processing center. It is important to emphasize the fact that such systems pose very high processing cost, total cost of ownership, and maintenance cost. Unfortunately, the expenses are being billed to the bank accountants. Different user interfaces, different terminologies all are confusing factors for bank users who have different backgrounds. Therefore, the majority of customers prefer visiting bank offices rather than using the Internet. This fact may also bring negative impact on bank incomes, where customers will have to change to banks with wider office distributions and better service facilities. Operations at offices are costly and, naturally, each new branch office brings along additional costs.

Another important shortcoming with current system is that employee monthly payments of a firm have to be done via the bank of the firm’s own choice without consulting the users argument. This monopolized enforcement is contradicting with the internationally recognized consistency property of e-payment systems and the fundamental human rights.

There are, recently, various ongoing activities for defining policies, functions, architectures, and protocols used in financial information exchange. The **Financial Information eXchange (FIX) protocol** is a messaging standard developed specifically for the real-time electronic exchange of secure transactions. As stated by the FIX consortium, FIX is an open message standard controlled by no single entity, that can be structured to match the business requirements of each party.

The existing e-payment structure is merely a conglomerate of discrete and dedicated payment services. In fact each bank has its own Electronic Fund Transfer (EFT) system, in which, every transaction has to go through four processing nodes on the Internet. These nodes, as assumed, are the source node, intermediate nodes, and the destination node. The intermediate nodes play a central role, where each node has its own central payflow processing facilities established for their own branch offices. This fact is illustrated in Fig.1. With the current operational model, at any given time, a matrix of randomly occurring processes is created, which can be given by:

$$\begin{bmatrix} SRC_1 \Rightarrow HQoS_1 \Rightarrow HQoD_1 \Rightarrow DST_1 \\ \vdots \\ SRC_n \Rightarrow HQoS_n \Rightarrow HQoD_n \Rightarrow DST_n \end{bmatrix} \quad \begin{array}{l} HQoS = \text{Head quarter of source} \\ HQoD = \text{Head quarter of} \\ \text{destination} \quad SRC = \text{Source} \\ \text{(sender)} \end{array}$$

The matrix of operations depicts the fact that each transfer will, at least, traverse through four nodes, the source, the source head quarter (HQoS), the destination head quarter (HQoD), and the destination node.

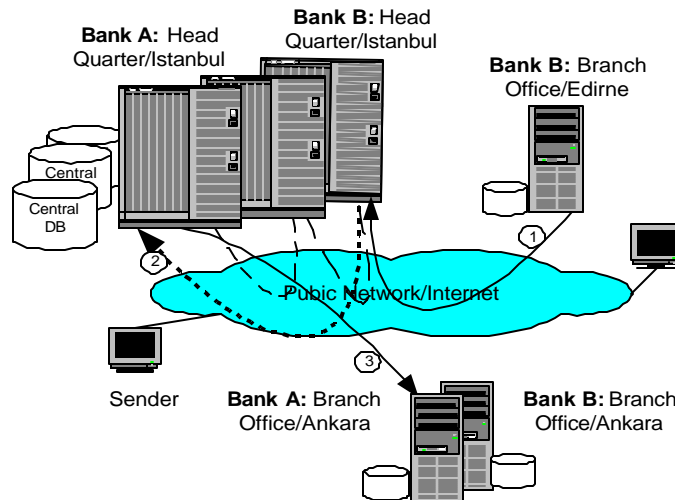


Fig. 1: Current e-payment architecture

This system introduces two major disadvantages, ineffective use of Internet bandwidth and other computing resources, and increased security risk figure. Internet traffic rate during office hours is very high. Under conditions of high load and congested Internet traffic, the possibility of completing a transaction is very low. In general, Internet infrastructure services are poorly configured or ineffectively operated. However, this is not only the reason for latency in this cumbersome transaction processing, in addition, the banks themselves provide very low line capacity for their Internet services, which should urgently be increased. To increase the Internet bandwidth requires additional costs that might as well be reflected on customers budget.

On top of these important shortcomings, each business, employer, or any counter-party dealing with payment, enforces the use of its own e-payment system, in which a bank will be appointed through which the payee will receive the payments. For a particular case, this means that, each time an employee changes firm or moves to another community, he or she must deliver a completely new bank account to the new firm, if non existing from before. This is also true for a B2B payment case, where the receiver will always have to choose the bank on payer's premises. Unfortunately, regulations for many individuals acquiring a new bank account do not provide reasonable means to solve this problem. Why not using own bank instead of being manipulated or forced to choose the bank chosen by anyone else? With the new e-payment architecture we help, in first place, to solve this monopoly problem. As shown in Fig 1, Istanbul city hosts all of the head quarters, which in itself a conflicting situation. Istanbul has one of the most inefficient and unstructured Internet infrastructure in the world. This, in turn, worsens the Internet traffic up to a saturated and highly congested state during rush hours, in which bank web servers are in complete deadlock state.

III SUGGESTED SYSTEM

Integration of national regulations that comply with the European Union standards will have a significant impact on the development and adoption of electronic payment systems in Turkey. There are a number of activities [3] in standardization that will hopefully be reflected on the Turkish e-payment and transaction arena. As ever, banks have been enthusiastic in their own home made approaches and have been eager to experiment with different solutions.

As stated earlier that the existing transaction systems have shown numerous shortcomings, where the potential problems are mainly related to the monopolized, opaque structure, which was heavily influenced by locally developed approaches of the banks themselves. Alongside SET [5], more lightweight mechanisms have been introduced to both simplify and reduce the cost of Internet transactions, without adversely affecting security and fraud concerns.

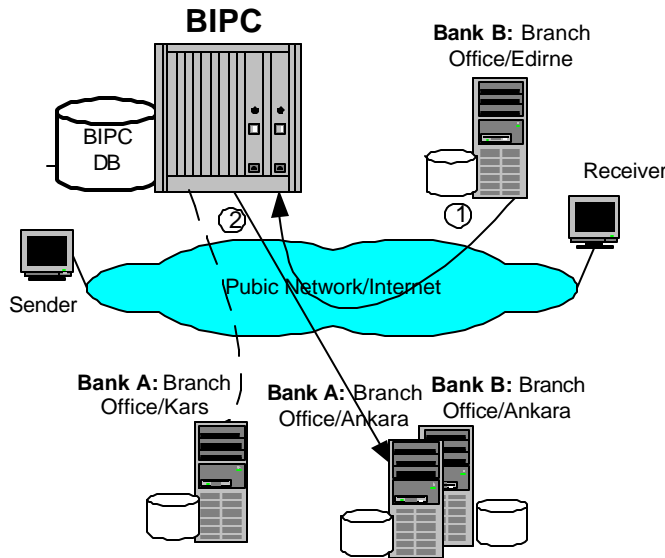


Fig. 2: BIPC's transaction architecture

As shown in Fig. 2, BIPC is designed to function as an account-based transaction system, which associates every user with an already established bank account. The entire architecture is mainly aimed to solve problems introduced inherently in the existing payment system, some of which are summarized as:

- *Atomicity*: The transaction must occur completely or not at all,
- *Consistency*: All parties must agree on the facts of the exchange constraints, e.g., receiver should not change banking relations on senders premises,
- *Economy*: Conducting a transaction should not be expensive,
- *Interoperability*: The system must support interaction between different systems,
- *Code reuse*: Object-oriented approach to allow code reusability.

A. Basic Requirements

The existing e-payment infrastructure should have been implemented with the properties mentioned above. Especially, the Consistency and Economy properties drew an import attention in the design of BIPC. Interoperability with major payment systems and e-commerce systems has been considered as an important matter while developing BIPC.

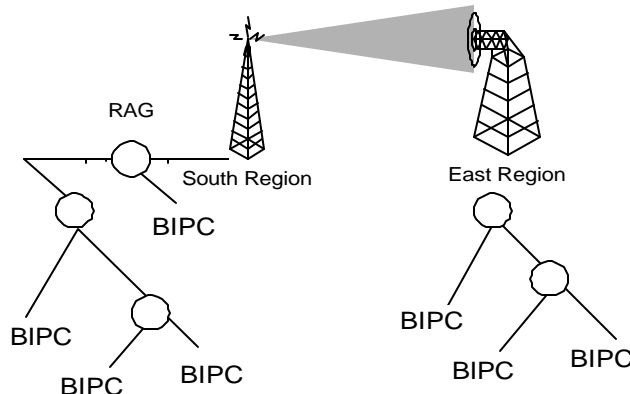


Fig. 3: Hierarchical BIPC's architecture

Integrating various types of payments and transactions, such as from firm to employee, from bank to bank, assurance companies, financial institutions, and from customers to merchants. Bearing these features in mind, BIPC should also satisfy the following requirements:

- *Scalibility*: One should add new payment and transaction systems and transactions types without having to install new software or perform additional modifications.
- *Flexibility*: One should, at any time, be able to change banking relations and continue to use existing systems.

B. Proposed National Payment Backbone

The proposed approach, shown in Fig.2, aims to remove the main obstacles, i.e., the head quarter nodes, from the current architecture shown in Fig. 1. Alongside BIPC, we suggest a technical approach to the national e-payment system, whose main objective is streamlining the ever-growing trading processes carried over the Internet. BIPC, comparing to the current system, introduces several advantages some of which are higher performance related to minimized latency, security, and open system approach in order to remove monopoly of property approaches. The architecture of the prototyped BIPC is comprised of:

- *Clients*: Web browsers,
- *Servers*: Payment and transaction gateways,
- Originators and receivers *bank accounts*,
- Originators and receivers *BIPC accounts*,
- Traders,
- Merchant acquirers,

C. Hierarchical Payment Backbone

To spread the Internet based payment services we need to establish a more efficient structure. Due to geographic disperse and different technological infrastructures, regions exhibit different performance figures for their Internet infrastructures. In order to solve problems associated with the different infrastructural approaches, we configure regional payment services into a single core network. For this architecture, Regional Autonomous Gateways (RAGs) will play the major role, which will function as regional bridge between two neighboring BIPC's. Fig. 3 shows RAG connections.

IV CONCLUSIONS

We have introduced the policy, procedures and architecture, and shortcomings of the existing e-payment system. It has shown two obvious concerns, the opaque policy and ad hoc technical approach, and the monopolizing banking and customer policy. Because of the payment architecture and procedures, fund transactions take, in average, an entire day to settle. If, for example, we attempt today to pay a debt with a deadline of tomorrow, then we are late out and will have to pay a penalty for the delay, which was introduced by the transaction processing system of the bank. Another unsound characteristic is the monopolizing banking policy, which forces employees to open accounts in payer's banks. These two disadvantages can be removed by deploying the BIPC. That is, BIPC is considerably faster, more reliable, and scalable than the existing solution.

BIPC allows payment processes to be initiated from user browsers of any kind without the need of any additional client component. All necessary components are installed on the BIPC's and banks servers

without worrying about the underlying technology. The payment information can be encrypted by an SSL set up between the users Web browser and the BIPC's server, and between the BIPC's server and the bank's server. In this structure SSL certificates form the necessary trust channel between Web browsers and BIPC servers. Approved SSL server certificates satisfy the need for confidentiality, integrity, authentication, and nonrepudiation.

The prototype of BIPC is implemented in PHP, which has brought the advantage of object-oriented design to ensure efficiency in both programmers' time and deployment time. Though, we only implemented bank-to-bank and firm-to-bank modules, we recognized the advantage of software reuse, easy integration with existing technologies, and security enforcements. A Public Key Infrastructure (PKI) supported version of the entire project will be delivered in a short due, which is designed to incorporate security measures by combining digital signatures with X.509 digital certificates. For example, consider the case of secure payment transaction that takes place when a user visits BIPC's site to issue a debt payment. When user's browser accesses BIPC's server, a public key from the server has already been delivered to the client browser as an X.509 digital certificate. It is required that, the certificate is signed by an approved authority, and the signer's public key is already embedded in the browser software itself. Issues with establishment of trusted certification authorities, and distribution of certificates are addressed in [7].

REFERENCES

- [1] Financial Information eXchange (FIX) protocol, Version 4.3, 09.20.2002, <http://www.fixprotocol.org>
- [2] Electronic Payment Standards Organization, <http://www.diffuse.org/payment.html>
- [3] European Communities' Electronic Money Directive, http://europa.eu.int/lex/pri/en/oj/dat/2000/l_275/l_27520001027en00390043.pdf,
- [4] Bank Internet Payment System (BIPS), <http://www.fstc.org/projects/bips/spec/license.cfm>,
- [5] Secure Electronic Transaction (SET), <http://www.setco.org/download.html/#spec>,
- [6] European ePayment Systems Observatory (ePSO), <http://epso.jrc.es/>
- [7] Kondakci, S, Evaluating the E-business Trust Infrastructure of Turkey, in press IT Consortium of Turkey, December 2002.