E-BANKING – DEVELOPING FUTURE WITH ADVANCED TECHNOLOGIES

Lj. Antovski, M. Gušev

Institute of Informatics, Faculty of Natural Sciences and Mathematics,
Sts. Cyril and Methodius University,
Arhimedova bb, PO BOX 162, Skopje, Macedonia
{anto, marjan}@ii.edu.mk

Abstract: Internet forces are affecting the banking sector transition more than any other financial provider group. E-Bank solution should deliver three key requirements: High Availability, Scalability and Security. End-to-end security consideration includes network security, data integrity and identity authentication security. Framework architecture for multichannel B2C solution enforced by reliable Network and N-Tier architecture is proposed. The architecture is designed to fulfill the key requirements.

Keywords: e-bank, scalability, security, availability PKI, B2C, N-Tier, networking

1. Introduction

The advent of E-Business, technological innovations and globalization are increasingly driving businesses to change their traditional modes of operation. The Internet offers many opportunities to financial services providers. The financial institutions are starting to use the Internet for interaction with users, in addition to 'traditional' transaction banking.

The electronic banking environment must be built with the same attention to detail and architectural sophistication as the physical space in which people use the financial services. The users exhibit an extreme form of electronic channel usage, leaving the designers only a precious seconds to present and sell their content.

Banks are financial institution, which are not designed to sustain the shift to electronic dealing in a fast and secure manner. The raising trend in the world is the outsourcing of electronic services to IT companies which have technical and human resources to maintain QoS (quality of service) of the multi-channel architecture.

2. E-bank Service Requirements

A successful E-Bank architecture requires a merged approach combining expertise from both the network and application development camps. Experience has proven that keeping network operations and application development as separate disciplines does not work.

In order to deploy a successful E-Bank implementation, one must address three key characteristics of the service: high availability, scalability, and security. A solid E-Bank solution will only be achieved through an architecture that meets these requirements across the network, the service channels, the database, and the server's operating system.

High availability is the ability to provide continuous access to E-Bank services for the clients. To deliver these E-Bank services successfully, high availability must be maximized across all layers of an infrastructure.

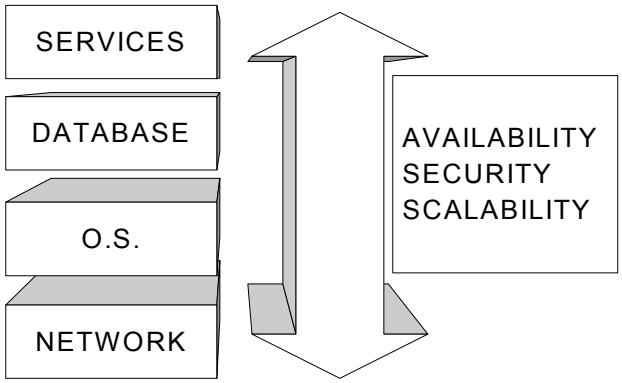

Figure 1: E-Bank Service Requirements

The right network design ensures there is no failure that will impact the high availability of the overall system. Designing for high availability includes the elimination of any single point of failure by providing redundant network devices and network paths.

High availability can also be achieved at the operating system, system services and application code layers through a mixture of server redundancy, rescue and failover scenarios.

Scalability is associated with performance enhancements, such as increased CPU speed, increased network bandwidth, etc. Consideration must also be made for supporting a large number of simultaneous user sessions and financial transactions. Scalability must be addressed across all facets of an E-Bank infrastructure.

Scaling an E-Bank site can be achieved by either scaling-up (bigger servers) and/or scaling-out (more servers). The choice is on what one would like to achieve because scaling-up takes advantage of increased hardware capability while the multiple servers in a scale-out solution provide redundancy, which means higher availability.

Channels should engineer for the virtually limitless capabilities of scaling-out while maximizing the benefits of scaling-up. This results in smaller initial software and hardware investments, which can be expanded as the business grows.

Security is a major consideration for the E-Bank infrastructure. As the nature of an E-Bank network is to conduct financial transactions, it becomes a likely target for malicious activity originating from the Internet community at large. Strong security consideration should include the following steps:

- Network Security
- Data integrity and privacy
- Identity security
- Security monitoring

3. Security Consideration

Security is a major aspect of an E-Bank solution. The effect of any sort of security leak in the E-Bank service will be a substantial loss of business. However balance should be achieved between security and usability of the services offered by the e-bank center. The design is in such a way to implement a sufficient security solution, good performance and ability to extend additional security if required. The best security solution implements measures that branch out from network to service components layer

3.1 Network Security

Network security is a leading link in the security chain. The three main networks components of an E-Bank security solution include:

- Extended Access Control Lists (ACL) on routers
- IOS Firewall Feature Set (FFS)
- Secure Stateful Firewalls

Routers provide in initial line of defense against extraneous traffic entering the E-Bank network. Tight Extended ACLs are applied to the inbound interfaces to the routers. These ACLs need only to allow traffic that is relevant to the E-Bank center. Although several TCP/UDP ports may need to be permitted using ACLs, other traffic such as PING, Telnet, and FTP are not required and should be de-

nied. No login ability to router from the 'outside' network should be allowed and one should use security technologies like SSL/Kerberos and others to secure and account for access to the router consoles.

Firewalls provide a high level of stateful aware security between the front-end servers and the back-end database and application servers. Specific policies are installed to only allow communication between the front-end servers and the back-end database and application servers. Using address translation (NAT), the addresses of the back-end servers are hidden from the outside world. Only trusted stations known by the stateful firewall and authorized through a rule set to access the firewall's console.

3.2 Data Integrity and Privacy

The data integrity ensures an exchange of financial and other sensitive data between the bank and the customer in authorized and protected manner. Depending on the choice of the channel for data exchange, different levels of security are to be implemented. For instance, the Web channel is mostly exposed and the highest level of protection should be applied.

The employed security models in E-Bank solution are:

- Secure Socket Layer (SSL)
- Public Key Infrastructure (PKI)
- Identity Authentication

The current mainstay for securing web transactions is the Secure Socket Layer, or SSL. Secure Web Servers use the SSL protocol to create an encrypted communications channel between the client and server on the transport layer. SSL is a generic "pipeline" that secures data. It allows the client and the server, to negotiate cryptographic algorithms to use, provides a protocol for them to do the negotiation ("SSL handshake") and then exchanges data using the algorithms. Additionally, the server is authenticated to the client during the handshake.

The main steps in the SSL handshake are

- To determine the set of algorithms to use for the new connection;
- Authenticate the server to the client and to exchange random data to be used later for symmetric cipher keys, using the asymmetric cipher that was negotiated in previous step;
- Start sending data encrypted in the symmetric cipher.

The asymmetric keys are usually 1024 B long, while the session key is with length of 128 B. It promotes this protocol to be unbreakable in a lifetime period.

Though the SSL communication is secure, it suffers from certain drawbacks. The major concern is that it does not provide non-repundation on the information sent

because it is based on a random session key generated at the clients end. There is a need of implementing a whole structure in the case of financial transactions, where non-repundation is a key factor. On the application layer the Public Key Infrastructure (PKI) is introduced. PKI comprehensively satisfies the security requirements of e-bank:

Authentication

The customer requests the Registration Authority (RA) for a certificate.

- The Registration Authority validates the customer's credentials.
- After valid credentials are ensured, the RA passes the certificate request to the Certification Authority (CA).

Confidentiality

- The customer generates a random session key at his end.
- The session key is sent to the bank, encrypting it with the bank's public key.
- The bank decrypts the encrypted session key with its private key.
- The session key is employed for further transactions.

Integrity

- The message is passed through a suitable hashing algorithm to obtain a message digest or hash
- The hash, encrypted with the sender's private key is appended to the message.
- The receiver on receiving the message passes it through the same hashing algorithm.
- The digest he obtains is compared with the received digest. If the digests are same, it implies that the data has not been tampered with, in transit.

Non-Repudiation

- The hash is encrypted with the sender's private key to yield the sender's digital signature.
- Since the hash is encrypted with the sender's private key (which is accessible only to him), it provides an indisputable means of non-repudiation.

PKI, being a universally accepted standards compliant security model provides an establishment of a Trust chain, valuable in financial transactions.

Last major role in application security is Identity Authentication. The identity validation is established through various methods of identity check, depending on the channel one uses. The methods implemented are:

- User name and password validated on client's side with the use of the login media which encapsulates encrypted user information
- Cookies
- Digital Certificates stored on login media (smart cards or mini CD-s)

4. Network Framework Architecture

The e-bank network is consisted of following building blocks:

- Edge Routers
- Access Server
- Multilayer Switch
- Stateful Firewalls
- Servers

Edge Routers are located at the perimeter of the e-bank network and provide connection to Internet, Dial In services for the WAP (Wireless Application Protocol) and IVRS (Interactive Voice Response System) channel. It also provides Dial Out services for the Fax Channel. The Edge Router is the Access Server to and from the e-bank network.

The first line of security is implemented at the Edge Router. Security services are provided with the use of packet filtering extended Access Control Lists (ACLs) and dynamic Firewall Feature Set (FFS).

The Multilayer Switch provides core network switching of an e-bank network. It needs to deliver multilayer switching while meeting the requirements for security, scalability and high availability.

Stateful Firewalls are used to secure connections from front-end to back-end servers. They only allow restricted services from restricted servers to exchange data over the firewall. Only the Web and WAP server could push/pull data to the servers in the back-end network.

In the framework, there are different types of servers implemented. They meet the requirements for scalability, especially for scale-out or scale-in. The WEB and WAP servers are equipped with additional set of memory, processors. These servers sustain the largest amount of users load. The other servers in the network, the dispatcher's servers and adapter server are with modest characteristics.

The Data Store Server houses the data for the e-bank center. To ensure scalability, this server is often scaled-up and implements failover clustering for high availability.

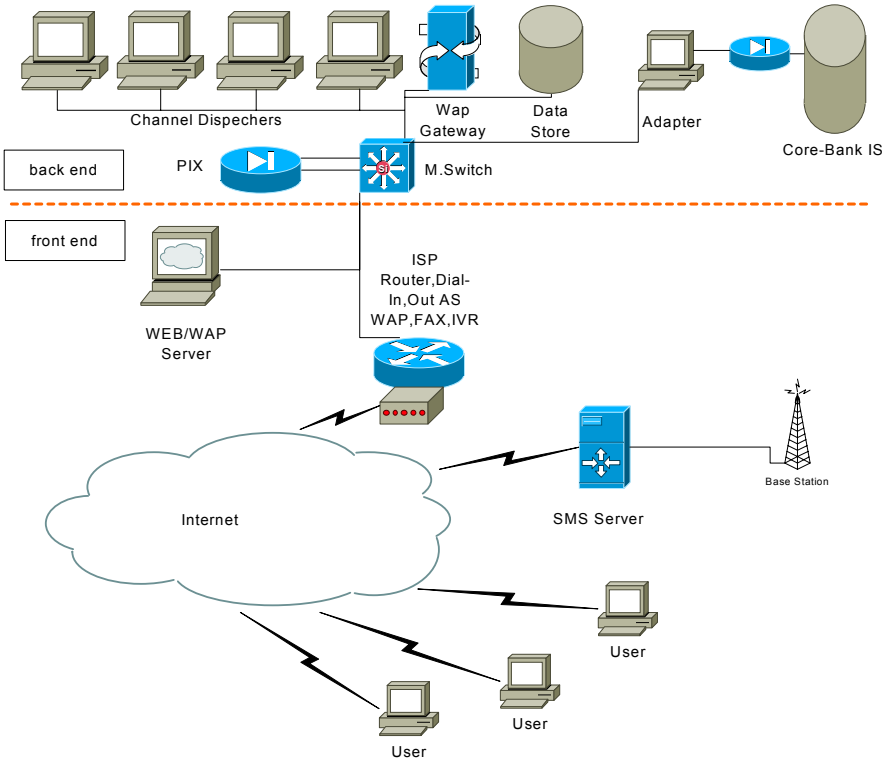

Figure 2: Network Framework Architecture

As Fig.2 shows, the network architecture is a single site implementation of an e-bank multichannel solution. It is consisted of a front-end and a back-end network. The network is virtually divided by the Stateful Firewall.

The front-end network consists of WEB server and WAP server. These servers are responsible for generating presentation services for the WEB and WAP channel. The front-end network is connected via Internet to the SMS server of the Mobile Phone Company. The users connect to the e-bank network through the Edge Router.

The back-end network is protected from intruder's attacks with the Stateful Firewall. It implements the Dispatcher Servers for different channels of services. For instance the Dispatchers Servers offer services for the Email, Fax and Sms channel.

The back-end network also implements a WAP gateway. This gateway is essential in a situation where the e-bank center is WAP service provider at the same time. With configured Access Server for WAP Dial-In, WAP gateway and WAP server, this framework offers a complete Mobile Internet Site Solution.

The Adapter Server is used for integration with the existing Core-Bank IS and its functionality will be discussed later in this paper.

5. N-Tier Architecture

To fulfill the above requirements for availability, security and scalability, an N-Tier architecture is proposed. This architecture is suitable for software development because it meets the request for project development with the following components:

- Open architecture
- Rapid deployment
- Workflow capabilities
- Separated content/presentation

The N-Tier application architecture is characterized by the functional decomposition of applications, service components and their distributed deployment. As shown on Fig.3, The N-Tier architecture consists of:

- Data Tier
- Data Access Tier
- Business Tier
- Presentation Logic Tier
- Presentation User Interface

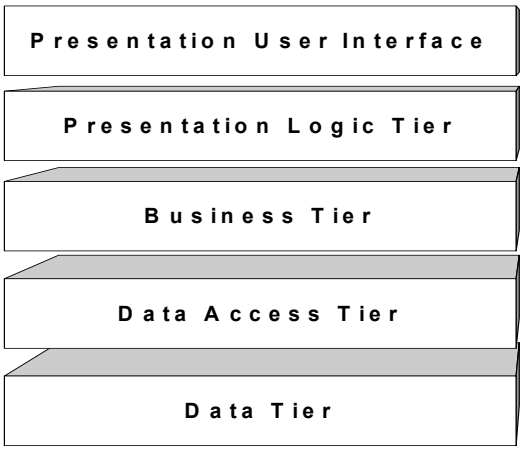

Figure 3: N-Tier e-Bank architecture

The Data Tier is the essential part of the architecture is. It is the Database Management System (DBMS) consisted of complex and comprehensive high-end

Database products. The required optimization is achieved through query optimization, indexing and precompiled stored procedures. No business logic is placed in this tier.

The Data Access Tier includes Interfaces with the databases. It includes objects that are to be used by the Business Tier, which encapsulate generic methods for connection and commands.

All the elements of business logic, business rules and data manipulation are placed in the Business Layer. It encapsulates common business logic for all the channels of the e-bank architecture. The services for authorization, authentication, notification, rules, transactions and schedule define the common business logic used by the Presentation Logic Tier and different channels of communication.

The Presentation Logic Layer provides an interface to the end user into the services offered by the e-bank. The data received from the Business Layer is transformed into usable and readable form for the user. The transformation differs for different channels. This Layer could also encapsulate a Proxy Tier, which enables applications from different platforms to communicate with the e-bank services through standard protocols for accessing remote objects, like SOAP (Simple Object Access Protocol). This is the Layer where the code for the WEB and WAP servers is placed, also including the services for Fax, Email and Sms.

The Presentation User Interface is physically on the client's side and it implements Web Browsers, Phones, Faxes, Mobile Phones etc. Additional transformation using scripts is accomplished at this layer. This stands for smart devices as Browsers, PDAs and Mobile Phones that allow scripting.

For this type of architecture asynchronous communication among the layers is essential. It would allow different layers to request data from another layer and continue working while the data is processed. The most suitable solution is the implementation of message queuing. Because this environment is highly distributed, asynchronous way of communication through message queuing is essential to maintain quality of service. This service should guarantee extremely fast inter-application communication, message delivery guarantees, sophisticated message and queue security mechanisms and queue location independence.

All the tiers communicate with the use of message queuing. The information is separated from the presentation and exchanged with the use of restructured XML messages.

6. Integration with existing Core-Bank IS

The integration of the e-bank architecture and the Core-bank IS of the bank is achieved with the use of adapters. The adapters offer services for connection

with the Core-Bank Database, system for transaction's processing and triggers that generate events in the system. These adapters support asynchronous processing suitable for huge number of simultaneous users.

7. Conclusion

The banks are now in a mature position and are being forced to change rapidly as a result of competition, customer demand and technological innovations. The power of Internet forces affects the banks now more than ever. To lower the costs and accept more demanding user the banks have to offer new electronic financial services.

The banks could not sustain the swift change in electronic services. The perfect solution is the outsourcing of the electronic services to well known IT companies that have resources to rapidly build new services.

These services require highest levels of security, scalability and availability. The security requirement is fulfilled only with comprehensive security implementation from network to application services.

Framework network architecture is proposed, which is secure, scalable and highly available. The N-Tier Software Architecture allows RAD (Rapid Application Development) and deployment with high availability, scalability through phase layer upgrades and PKI security implemented on Application Layer. The framework architecture proposes a model of future proof solution for building an e-bank center.

8. References

1. Gušev, M. (2001), "Tools for digital age", *Proc. of SEE Conference on Digital Economy*, Skopje, 21-22 Jun.2001.
2. Gušev, M. (2000), "E-Commerce, a big step towards E-Business", Proc. of 2nd SEETI Conf. on Trade Initiative and Commerce, Skopje, Macedonia, 8 Nov. 2000.
3. Edward, T. (2001), Transactional COM+- Building Scalable Applications, Addison-Wesley, London.
4. Elison, C. and Schneier, B. (2000), "Ten Risks of PKI: What You Are Not Being Told About Public Key Infrastructure", Computer Security Journal, Vol.16, N.1, pp.1-7.
5. Freier, A., Karlton, P. (1996), "The SSL 3.0 Protocol", Specification, Netscape Comm. Corp.
6. Howard, M. (2000), Designing Secure Web-Based Applications for Windows 2000, Microsoft Press, Washington.

7. Microsoft and Cisco (2001), "E-Commerce Framework Architecture Document", White Paper.
8. Milosevic, A. (2000), "Multi-Channel Bank Information System-Bases, Architecture, Integration in Existing IS", Proc.of New Banking Vision Conf., Ohrid, 21-23 Feb.2001.ed. Mircetic M., Pexim, Skopje, pp. 61-67.
9. Milosevic, A. (2000), "Multi-Channel Bank IS", Proc.of Bankinfo Conf., Belgrade, Sep.2000.
10. Milosevic, A. (2001), "Path to successful E-Banking Solution", Proc.of Infotech Conf., Belgrade, Jul.2001.
11. Rivest, R., Shamir, A., Adleman, L. (1978), "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Feb.1978 Vol.21, pp.120-126.
12. Sun Microsystems (2001), "Scaling the N-Tier Architecture", white paper in Solaris Infrastructure Products and Architecture, Sun, Palo Salto.
13. Terplan, K. (2001), OSS Essentials-Support System Solutions for Service Providers, Wiley, Canada.
14. Unnithan C.R. and Swatman P.M.C. (2001), "eBanking Adaptation and dot.com Viability ", to appear in the Proc.of BIT'2001 11th Annual Business I.T. Conf., Oct.30-31, Manchester.