Security for SEPA Bank Servers in A Cloud Environment

Master Thesis in Information and Communication Systems Security

SALMAN KHAN

Master's Degree project
Stockholm, Sweden 2013

TRITA-ICT-EX-2013:5
Abstract

Due to Information Technology (IT) the world has become a global village. We can get information from anywhere on a single click. IT in banking sector connects banks with each other based on their location. Everyone in global world wants a quick response to any query they make. In Eurozone, within each country, banks are centralized and work very well at a national level. Problem arises when they do transactions outside the country, convert money to other currency, charge bank fee, the time it takes to complete the transaction, and much more. Business committee and ordinary person suffer because they want transactions to be completed within few minutes. Research is carried out on how to solve this issue. European Union took initiative to remove barriers, implement one currency system and connect member states. For this purpose EU launched a Single Euro Payments Area (SEPA) system to facilities people and businessman.

Our project focuses on development of such infrastructure, where we can provide solution for their problem. After initial study of this area, we found module for secure server in SEPA system. Therefore we configure appropriate servers, setup connections between them for communication with basic security.

After implementation of secure server’s platform together with other applications, we developed solution of cross-border transactions named SEPA secure banking, which is our area for banking system. We provide secure communications between SEPA servers in a SEPA secure banking system.
Acknowledgements

"In the name of Allah, the most Gracious, the most Compassionate"

First of all I would like to thank Allah Almighty who made me able to complete this important work. I would also like to thank TSLab, KTH for their resources, time and co-operation.

I would like to acknowledge the quality guidance given by my supervisor Professor Sead Muftic throughout the itinerary of the research. Without his support it would not be possible to complete this task. Great interest in discussions, meetings and feedback gave me right direction to my master thesis. Once again, Thanks Professor for such wonderful and constructive time.

Finally, special thanks to my family for their prayers and support. Some of my friends who helped me in my master project, I must mention the names of Sheraz Altaf, Ikram Rahim, Muhammad Farooq Afridi, Muhammad Raza and special thanks to Naser Saeed Awan (lala) who always motivated me at the right time.
Abbreviations

IBAN International Bank Account Number
IDAMS Identity and Access Management System
PCI Payment Card Industry
PDP Policy Decision Point
PEP Policy Enforcement Point
PIN Personal Identification Number
POI Point of Interaction
PTS PIN Transaction Security
SAML Security Assertion Markup Language
SCT SEPA Credit Transfer
SDD SEPA Direct Debit
SEPA Single Euro Payment System
SLA Security Level Agreement
DSS Data Security Standards
ECB European Central Bank
EPC European Payment Council
IBAN International Bank Account Number
IDAMS Identity and Access Management System
List of Figures

4.1 Secure SEPA System Design
4.2 Overall Security Architecture
4.3 Portal Security Server Architecture
4.4 Banks Servers
5.1 Secure Cloud Banking Main Page
5.2 Cloud Secure Banking Login Page
5.3 Cloud Banking Admin Portals
5.4 SEPA Administration Portals
5.5 Add Bank to SEPA
5.6 Registration Form
Contents

Abstract ........................................................................................................................................... 1

Acknowledgements .......................................................................................................................... 2

Abbreviations ................................................................................................................................. 3

Chapter 1 .......................................................................................................................................... 7

Introduction ...................................................................................................................................... 7

1.1 Introduction ............................................................................................................................... 7

   1.1.1 Audience ............................................................................................................................ 8

   1.1.2 Prerequisites ....................................................................................................................... 8

1.2 Research Methodology .............................................................................................................. 8

1.3 Motivation and Scope ................................................................................................................ 8

1.4 Outlines of the Thesis ............................................................................................................... 9

Chapter 2 .......................................................................................................................................... 10

Single Euro Payment Area (SEPA) System ..................................................................................... 10

2.1 SEPA Credit Transfer Transactions ......................................................................................... 10

2.2 SEPA Direct Debit Transactions .............................................................................................. 11

2.3 Security Features and Requirements of the SEPA System ...................................................... 11

   2.3.1 Data Protection .................................................................................................................. 12

   2.3.2 Card Security ..................................................................................................................... 12

   2.3.3 Terminal/ POI Security ....................................................................................................... 12

Chapter 3 ........................................................................................................................................... 14

Financial Transactions ...................................................................................................................... 14

3.1 Cross-Border Payments ............................................................................................................ 14

   3.1.1 Migration to SEPA System ............................................................................................... 14

3.2 Elements Used in SEPA Transactions ..................................................................................... 15

   3.2.1 International Bank Account Number ............................................................................... 15

   3.2.2 Business Identifier Code ................................................................................................. 15
Chapter 1

Introduction

1.1 Introduction

In this era of global village when the world is getting smaller and smaller, people want to have as much resources as they can within their reach. The only problem that most of them face is the expense through which those resources can be available for utilization and within ones reach. That’s where banks play a vital role. They share those resources with everyone by giving out loans on easy instalments, but the most important player in this is the Internet. That lets us connect to this magic cloud, so we can access whatever we like in the virtual world. Our dependence on banks is not just limited to taking loans but it also helps us in our day to day life affairs, like paying utility bills, rents, mortgage, using ATM to draw out money, etc.

All these things put a lot of pressure on Bank Servers and since the operations require the highest level of security, it means they need to have good infrastructure to cater these requirements. Good infrastructure requires too much investment. This may not be a problem for large banks, but smaller ones do not have enough resources to invest for good infrastructure and they are bound to form alliances with other big companies to induct the required infrastructure that in return affects the pockets of the customers, who have to pay access to the banks, so that they may cover their costs. One of the major developments to rescue small businesses around the world has been the introduction of cloud computing and virtualization. That lets the service providers to offer cheap services via the cloud.

Currency variance is another aspect that banks have to consider for transfers from country to country. Some of the overheads can be eliminated if one can introduce a single currency and can be beneficial to the customers, since the tourists do not have to pay the conversion charges once they are visiting a country for shopping or leisure trips. SEPA (Single Euro Payment Area) is a very good solution that eliminates currency conversion problems.

SEPA or Single Euro Payment Area is an ongoing European Payment Councils (EPC) project to introduce Single Currency Transactions (EURO) within and outside Europe. As per EPC, SEPA relies on these main players: Public Authorities, Bank Customers, and the Banking Industry. We shall further discuss SEPA in detail in Chapter 2[1].
Single Euro Payment Area (SEPA) is European Union project on how to benefit their citizens and businessmen. General idea behind the project is to implement one payment system across the whole EU zone. This will enable euro payment across the euro easily, securely and quickly as they are in their own country. This payment system will change way of payment and help people who travel across the EU. My part in this project is to design and implement secure SEPA servers. We have different type of servers; Bank Server, which connect to National Server.

1.1.1 Audience

This Thesis addresses banking and IT industry professionals because of their valuable relationship within the development of the banking sector. In modern times IT has become one of the necessities of life and helps us in our everyday life, Modern banking sector is nothing without the IT industry due to emerging changes. IT has revolutionised modern banking system helping with the introduction of Visa Cards, Master Cards, ATMs and Online Banking etc.

1.1.2 Prerequisites

The prerequisites required to understand this research is to have at least a bachelor’s degree in Computers with a focus on servers, cloud computing. Basic knowledge in banking industry is required to understand some parts of this research, but to fully understand this research; one must have good knowledge about the cloud computing, security and servers. The reader should also have knowledge about the SEPA system and know how it can help the customers.

1.2 Research Methodology

The key factor behind this research is the method which drives the whole process. There are several types of research approaches e.g. Descriptive, Analytical, Applied, Fundamental, Quantitative, Qualitative, Conceptual, Empirical, etc. Depending on the type of research two basic approaches for research exist, i.e. Quantitative and Qualitative. We are using qualitative approach, which includes assessments, discussions and opinions [14].

1.3 Motivation and Scope

The Internet is growing at a rapid pace and after the introduction of smart phones the Internet traffic has increased very much. With new applications being developed and
businesses going online, the main concern that we face in today’s world is security. Similarly SEPA is a financial service that deals with customers and businesses; this is one of the motivations behind this project, since there is a big question about SEPA security from its consumers.

The main scope of this thesis is in the areas of IT, which needs up gradation for SEPA success. They include upgraded hardware to fulfil clients’ needs, introduction of SEPA cards, access to phone applications, online banking, etc.

1.4 Outlines of the Thesis

In this thesis we focused on deployment of web-servers, cloud infrastructure, and above all, security of the whole system. Organization of this report is as follows:

Chapter 1 is introductory chapter of the thesis. Chapter 2, brief descriptions of Single Euro Payments Area (SEPA) provide services and security requirements. In Chapter 3 brief descriptions of SEPA financial transaction, cross-border transactions, transaction requirements and elements use in transactions is given. Chapter 4 describes our Secure SEPA System design and Chapter 5 is about how we implemented different things, and a small demo. Finally, Chapter 6 summarizes what we can improve and enhance in the future.
Chapter 2

Single Euro Payment Area (SEPA) System

Single Euro Payments Area (SEPA) is an ongoing initiative of the European banking industry, making all electronic payments across the 32 countries in the European area as local payments, i.e. all national and cross-border transactions will be performed in the same way as domestic transactions. SEPA project is strongly supported by the European Commission and the European Central Bank. For the identification of accounts SEPA uses International Bank Account Number (IBAN) and Bank Identifier Code (BIC) by following all relevant ISO standards. Since SEPA has potential to support many customers by introducing SEPA cards, by improving GUI, and by introducing new delivery channels, thus requiring it to gain customer confidence, IT industry can help implement new security models and digital signatures, in order to reduce fraud and prevent attacks on ongoing transactions.

Banks would require new software SEPA packages. In a SCT session, initiator's id, receipt of credit transfer, how to support BIC and IBAN in a transaction and new message format according to ISO 20022 will have to be provided in one software solution. Other functionalities, like rejection or returns, also need updated software with these functions supported according to EPC standards and rulebook. Another big issue is the introduction of chips for SEPA cards that would provide ample opportunities to hardware vendors. In order to read SEPA cards development of fast processors with integrated systems to read SEPA cards (chips) is another opportunity to increase business.

2.1 SEPA Credit Transfer Transactions

Launched in January 2008 SEPA Credit Transfer (SCT) was the first step towards the implementation of ISO 20022 message standards. SCT performs transactions in Euros in 32 different countries without any charges or deductions. Customers are charged according to the agreed upon agreement with the Payment Service Provider. Customer has the opportunity to add 140 characters message with a transaction. In SCT the credit is transferred within two working days with a receipt of transaction as per SEPA rules. All banks under SEPA treats all transactions as local either national or cross-border. All active rulebooks and other documents associated for SEPA DD and SEPA Credit Transfer can be found on the European Payment Councils website [1].
2.2 SEPA Direct Debit Transactions

In November 2009 under SEPA Direct Debit (SDD) two schemes were launched. SEPA Core Direct Debit and SEPA Business-to-Business (B2B) scheme. I will focus on SEPA Core DD, since I am working on the consumer side, whereas SEPA B2B is a business product. SEPA Core DD is a mandatory product for all banks and on the other hand, SEPA B2B is optional. SDD is both creditor and debtor driven and uses a mandate for authorization. A mandate is a signed paper agreement of authorization that expires after 36 months.

Electronic mandate can also be generated and is called e-mandate. It can be issued to a customer using the same credentials that they use for online banking-mandate all three entities debtor, creditor and bank. Customer gets a billing form from the sellers website, provides account identification and other required information. Seller then transfers received e-mandate to customer’s bank. This way the customer gets his own bank website in order to prove his identity and account rights, thus giving confirmation of e-mandate to its bank and then rout to seller website again and they acknowledge the receiving of the e-mandate. The dealing with availability of e-mandates differs from bank to bank. The customer of a transaction signs a mandate and transfers it to the creditor in the creditor driven mode, thus laying responsibility on the creditor for collecting money from the customer’s account by storing original mandate, as well as other information for future. In the above model all the information is hidden from the bank, such as mandate signing and payment leaving the customer account, by means of mutual trust between the creditor and the customer. In case there is a problem with the transaction, SEPA reimburses the money within 8 weeks from the date of transaction. If fraud is suspected from the Customer’s end, the reimbursement can take up to 13 months. All payments made through SEPA are fully traceable.

The main difference between the Creditor driven and Debtor driven mode is that in the Debtor driven mode the signed mandate by the customer is kept with the customer’s bank instead of the biller, And the biller in order to get the payment has to contact the bank and after giving authorization (that is confirmed by the bank from the customer) releases the payment.

2.3 Security Features and Requirements of the SEPA System

Three different financial services i.e. SEPA cards, SEPA mobile and SEPA cash are available for the SEPA uses (SDD and SCT) bringing with them their own security risks
and requirements that need to be taken into consideration. EPC has discussed these requirements in security requirements book for SEPA single set of cards and terminal security. An overview of these considerations is as follows [11]:

2.3.1 Data Protection

Data protection to be ensured by EPC as per PCI DSS (Payment Card Industry Data Security Standards), there are certain requirements that need to be fulfilled according to PCI DSS council. The first requirement is to build a secure network infrastructure. That can be met using access control lists and firewalls. The second requirement is to use secure and different passwords for sensitive systems. This can be done by securing card holders information by using techniques such as masking, encryption and hashing, so that in case if hackers somehow do manage to get access to the encrypted data, they are not able to decrypt it since they won’t have the cryptographic keys.

Antivirus software must be deployed and regularly updated to counter against different threats. Application security should be considered of prime importance to develop trust between the cardholder and the organisation, that the cardholder knows that his information is safe with the organisation, Similarly the organisation must make sure that the cardholders access is given only to the relevant persons and to ensure that they must be provided with a unique identification and everything to be maintained in the logs. Access to every node and service in the network must be maintained where cardholder's data is placed. Keep on auditing the security systems and processes. Policies must be maintained in such a way that guarantees everyone security [11]. In case of shared hosting, providers must assure its capability to secure that environment in which cardholder’s data will be placed.

2.3.2 Card Security

According to the standards set by EPC, a smart card shall be able to select and initiate appropriate application, they should be able to communicate with the terminal for online authentication purposes and should generate unique certificates bind to every transaction in order to avoid transaction modification attacks exhibit lowest duplication of authentication certificates. Authenticate the right cardholder during a transaction and block a card if the maximum number of failed attempts of PIN code is met. Counter denial of service attacks by continuously checking all the transactions itself

2.3.3 Terminal/ POI Security

To improve POI terminal devices security, EPC want to move security evaluation requirements for devices from local vendors approach to a unified evaluation approach. It is important that all device manufacturers must implement EPC security requirements for terminal/POT devices. To avoid ambiguity in the vendors’ case, EPC proposed to consider PCI POS PED 2.0 as baseline [10], PCI PTS 3.0 was considered as baseline by EPC later on latest version of PCI POS PED 2.0.
According to the SEPA environment, EPC adds some extra requirements which were felt missing in the PCI PTS 3.0. This is called EPC plus Requirements and jointly with PCI PTS 3.0, these complete EPC Security Requirements for Terminal/POI devices. To use device in the SEPA domain, vendor of the device need to get a "SEPA wide Certificate" to prove the security. The unified security approach can be achieved this way and EPC will be sure card in SEPA will be processed in the same and secure way.

The following requirement of the EPC model should be fulfilled by POI devices to prove a claim to be secure device.

**Physical Security:** Every device should have at least two security approaches one is operative and other is used as backup. The device must have the ability to erase sensitive data like in the case of attack cryptographic key from the machine. The device must be capable of bearing alternate environmental and operational conditions. If there is any problem in the PIN, all digits should sound the same to avoid any security compromise.

**Logical Security:** Logical security of the device is almost of same importance as physical security. On the start-up logical security of the device includes self assessment of integrity and authenticity. The device should be updated before the firmware cryptographic authentication. The device should be capable behave normal and deal with such thing in the good manner in the case of any input (e.g. command or other entry). In the original digital form the PIN entered should not visible and after successful completion of transaction or time out in transaction device should automatically clear the buffer.

To minimize security risks number of attempt on the sensitive data must be limited and access to cryptographic keys, PIN and password both require authentication. Follow the standards like ISO 11568, ANSI TR-31 and TDEA to implement technique in the device, vendors will ensure that device will handle different keys with different values. Data will never print in the clear format and entry of transaction data and PIN code data should be handed separately [11].

Terminal/POI security has many other concerns e.g. IP and Link Layer (IPLL), IP protocols (IPP), Security Protocol (IOSO), IP Services (IPSV), Account Data Protection, Online PIN Security, Offline PIN Security, POS Terminal Integration Security, During Manufacturing, Between Manufacturer and Initial Key Loading [11].
Chapter 3

Financial Transactions

3.1 Cross-Border Payments

All over in the world currency is attached to a country. In country all banks are linked to each other and run on the same principle that payments process can perform easily and smoothly throughout the county. Europe is different: 17 countries share the same currency and it will expand further. Inside Eurozone, banking networks of different countries are not linked to each other and do not follow the same principle, that’s why payments within each of the Eurozone member states are easily and smooth, but payments across the national borders are not. These introduce SEPA Credit Transfer Scheme, SEPA Direct Debit Scheme and SEPA Cards Framework. Nowadays Eurozone runs dual systems; the traditional one will be soon replaced in by new SEPA system, not only for the cross-borders payments, but for all type of payments. In the Eurozone the payments across the national borders should be as easy as within the Eurozone separate countries. We achieve this because of SEPA. If someone wants to do business in Eurozone needs one bank account to conduct business throughout the zone [1].

Cross-border payments in the zone remove the difference in charges for cross-border and national payments in euro. SEPA implements euro in all EU member states. The main concept of SEPA is that charge for payment transactions offered by banks must be the same whether the payment is national or cross-border. In cross-border payments all electronic process includes, like credit transfer, direct debits and withdraws money to ATM [3].

3.1.1 Migration to SEPA System

In March 2012 European legislators adopted Regulation No 260/2012, commonly referred to as the “SEPA migration end-date regulation”. It defines the rules for the beginning, processes the credit transfer and denominated of direct debits in Euro in the European Union. The timeline specifying defines by the regulation when these rules will be implemented in all Member states. The Euro implementation deadline is 1 February 2014 and the deadline to denominate Euro payments in non euro area countries will be 31 October 2016. After these dates, present setup in euro credit transfer and direct debit will be replaced by SEPA. All countries must ensure that migration to SEPA instruments is conducted in accordance with regulations. However national timelines maybe longer or shorter than at the general European level, the migration and requirements deadlines maybe vary from country to country during transitional period. At 2016/2017 the transitional period will be end for all requirements [4].
3.2 Elements Used in SEPA Transactions

Same rules and standards for retail credit transfers and direct debits are denominated in Euro. All the rules are stipulated by regulation and set standard for all credit transfer and direct debits denominated in euro within the EU, where service provider is located in EU.

3.2.1 International Bank Account Number

After February 2014, the International Bank Account Number (IBAN) will be used for identification of account in national and cross-border payment in Euro within the EU.

3.2.2 Business Identifier Code

User can ask for Business Identifier Code (BIC) to provider until 1 February 2014 for national payments and 1 February 2016 for cross border payment. The BIC will be eliminated by Member states for national payment transactions until 1 February 2016.

3.2.3 ISO20022 XML

The ISO20022 XML message standard is mandatory between payment service providers. A huge transmission of credit transfers and direct debits in Euro by business users that are not microenterprises.

3.2.4 Free Choice of Payment Locations

Users can not be restricted in choosing from which account in Europe he will make credit transfer or direct debits in Euro. Neither provider will be forced to receive credit transfers or direct debits in Euro in an account located in a specific country.

3.2.5 Additional Debtor Protection Measures for Direct Debits

Customers give instructs to payment service provider how to handle incoming collection by specific billers. Provider will be then black listed or white listed of billers set amount specification. They will block other direct debit collection from their payment account.

3.2.6 Multilateral Interchange Fees

Multilateral interchange fee (some member sates service provider applied individual direct debits) will be removed on 1 February 2017 for direct debits in Euro from national payments and on 1 November 2012 for cross-border payments [4].
3.2.7 Principle of Equal Charges

Service provider must apply equal charges for payment in Euro within country or cross-border within the EU (Regulation No 924/2009). This principle of equal charges has been reinforced by the SEPA migration end-date regulation which has eliminated the €50,000 ceiling under which equal charges could previously only be applied [4].

3.2.8 Important Deadlines of SEPA System

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>31 March 2012</td>
<td>Eliminate 50,000 Euro ceiling for equal charges to apply, Pan-European reachability and Regulation No 260/2012 entered into force.</td>
</tr>
<tr>
<td>1 November 2012</td>
<td>Remove multilateral interchange fees (MIF) for direct debits on cross border transactions.</td>
</tr>
<tr>
<td>1 February 2014</td>
<td>Deadline migrate to SEPA credit transfer and direct debit within the Eurozone and no Business Identifier Code (BIC) is required for domestic transaction.</td>
</tr>
<tr>
<td>1 February 2016</td>
<td>For cross-border payments, BIC is not used products migration completed.</td>
</tr>
<tr>
<td>31 October 2016</td>
<td>Deadline for non-euro area countries for SEPA credit transfer and direct debit.</td>
</tr>
<tr>
<td>1 February 2017</td>
<td>For Multilateral Interchange Fee (MIF) will be eliminated for direct debits on national transaction.</td>
</tr>
</tbody>
</table>

3.3 Infrastructure

Initially SEPA foresaw the creation of a small number of competing hubs to process all transaction in the Eurozone and together all nation clearings. Round about 10,000 separate banks are together in this area. A Pan-European ACH (PEACH) is hub with connections throughout Europe; it has the ability to reach every bank in each SEPA country. PEACH also known as STEP 2, based near Milan and operated by EBA is currently processing an increasing number of cross-border transactions. Now in STEP2 (Feb 2011) has 117 direct participants and indirect participants are 5600 financial institutions. In domestic transactions the same facility are processed, because increasing number of countries [5].

3.3.1 Clearing Cycle

From 1/1/2012, ACHs and PEACHes will be required to operate in a manner which supports the requirements that credit transactions should be available in the customers account on the day following the entry of the transaction at the bank of origin [5].
Chapter 4

Secure SEPA System Design

In this chapter we discuss design of secure SEPA system which is developed to provide secure cloud banking services. Secure SEPA is part of Secure Cloud Banking project, use as application which interacts with cloud central security servers for authentication and authorization services. SEPA system has three different modules with respect to its architecture. They are Client module, server module and SEPA portal module. In this research we focus how to secure server module.

Figure 4.1: Secure SEPA System
4.1 SEPA System Architecture

The main focus of the project is security and integrity, that’s why we use Authentication, Authorization, and Accounting security architecture. It is an important feature of the system to check users before they join the system and authorization of resource access before a user starts utilizing it. The Figure shows an overall view of the portal security architecture and central security architecture and communication links between both architectures before providing access to SEPA resources.

Figure 4.2: Overall Security Architecture
4.1.1 Central Security Servers

Figure 4.2 shows overall security architecture of SEPA system. All the servers involved in central cloud security, in Secure Banking project we don’t cover central cloud security but we cannot be separated from SEPA as SEPA portal security is directly dependant on IDMS and SAML/PDP servers of the central security system.

![Diagram of Central Security Servers]

**Figure 4.3: Portal Security Server Architecture**

4.1.2 Portal Security Server

SEPA is available as web service for the users in the secure cloud system. The users are administrators (portal admin and SEPA admin) and use SEPA administration portal for multiple tasks. SEPA administrator in our system hierarchy is responsible to add users (bank admin) for bank and also assign roles for them. Other component of portal security has web server, VPN, PEP server and proxy server, as shown in Figure 4.2.
4.1.2.1 Web Server

We use web server as computer application in this architecture, providing web interface of the SEPA system to the users. To secure communication between clients and servers use SSL protocol. We use HTTPS, to avoid man-in-middle attack in SEPA system and web site authentication is also ensured. Due to HTTPS, communication on both sides is encrypted, which helps SEPA system in security by avoiding tampering, forging and eavesdropping attacks to some extent [6] [7].

4.1.2.2 Virtual Private Network

Administrators can only use SEPA system portal (portal admin and SEPA admin) who also have access to bank interface. Banks use their own security parameters on virtual a server, that’s why communication between SEPA cloud and bank servers we are using Virtual Private Network (VPN) technology to ensure secure communication. User can access this communication after successful user login and verification of resource access authorization.

4.1.2.3 PEP Server

To control access to resources Secure SEPA system use policy based control. Architecturally policy control has two main elements, Policy Enforcement Point (PEP) and Policy Decision Point (PDP). PDP server stored all policies and PEP initiates request/response sequence with the PDP server to make decision based on the policy stored in the PDP server. In the request message of PEP about resource (version, hardware/software) is send to PDP Server and in response checks all resources relevant policies (allowed or not) and it sends response message to the PEP server [7].

4.1.2.4 Proxy Server

Proxy server in SEPA system increases system security. Two main reasons to use proxy server in SEPA system, security, and proxy server hide IP address of original server and show IP address of proxy server is visible to outside users. Second is cache, which helps the user to speed up resources access. We can also configure proxy server as firewall after maintaining a login order to block specific ports and IPs.

4.2 SEPA Bank Server

Bank servers are organized in a hierarchical structure in the SEPA system, shown in Figure 4.4. We have two types of servers in SEPA system: one is National SEPA Server and the other is Bank SEPA Server. First, traffic come to Bank SEPA Server; check traffic IP address, if its match local IP address, then traffic is locally handled otherwise it is sent to National SEPA Server. National SEPA Server will communicate with Bank SEPA servers in case of cross-border transactions.
4.3 SEPA Customers

In SEPA system we have two types of customers (clients/users): mobile clients and web clients. For communication both of them initially use web pages via web server, which is under portal security administration [9].

4.3.1 SEPA Mobile Wallet

In SEPA system mobile client services is call SEPA Mobile Wallet. Due to Mobile Wallet client can access SEPA system from anywhere via mobile device and can use the same card mentioned in SEPA Web Wallet.

4.4 Security Services

The following security services are provided by SEPA system for all users, like administrators and bank users.
4.4.1 Authentication

At the begging in SEPA system all SEPA servers authenticate user in order to check whether username and password exist or not. If the username is correct, then user can get access to system. After the access to system, if user wants to access specific resource, SAML request-response exchange is performed with IDMS in the central security server for proper authentication and authorization.

4.4.2 Server Authorization

PDP is also part of the central security system of the cloud and PEP Server is part of SEPA portal security system. In authentication server, as discussed earlier when passes request to PDP/SAML server, both these servers generates a ticket with expiry duration. Ticket is then passed to the PEP server. After receiving the ticket, PEP then decided allows/reject the request for further processing in the system and user can allow getting access to specific resources in the SEPA system [8].
Chapter 5

Implementation and Demo

In this chapter, we will discuss how our system works. We will show pictorially how the administrator logins the system. After log in, he can assign roles, for example adding banking, deleting bank, registration of a client in the system etc. The system code is available in Appendix B. We are going to discuss this process below.

5.1 Contents Management System

For cloud infrastructure we used Content Management System (CMS) Made Simple 1.10.3. This is open source software to manage contents online which work on same for both operating systems (Windows and Linux). It is designed in PHP and to understand or work on it only requires basic knowledge of HTML and CSS. To run CMSMS setup it requires pre installed web server and pre configure database.

5.1.1 Windows: xampp

Linux is friendly operating system in engineering task as compared to Window. Adding database, configure Apache web server and PHP, all of them are totally different task and to complete them individual requires some time. After searching on Internet, we solve this problem of Window and found all in one solution. We find xampp which includes with Apache distribution combined with MYSQL, PHP, Perl and Apache web server in one package. It is easy in use, simple installer and can get all things working fine on local machine. In this project we use xampp-win32-1.7.4 on our machines before installing CMSMS on them.

5.1.2 CMSMS Setup

When installation of web server, addition of PHP and database is successfully completed. Then we install CMSMS on our local machine. To proceed with CMSMS setup, we need to put it setup under our webserver and create empty database using MYSQL and also empty file name config. PHP. After completion of this process, now user can type the following in the browser,

http://localhost/cmsmadesimplefoldername
and then user will get installation page of CMSMS to select language to use. To select in
the options user can precede the wizard. During the wizard it will ask about admin
account information for CMSMS and basic site name to manage contents. Then, it will
ask for the root username, password and also ask for database type are using. During the
installation, it will check all privileges needed and can also check the compatibility issues
and give error, if they find something wrong. If everything is ok, then it will display
success message.

5.2 Demo

We know that Secure SEPA Banking System is going to be part of online banking and
everything will be dealt online. Therefore, it is the main purpose of this research project
that it will have to be available online on the web. The client part will be accessible by
the general clients and users while the Admin part is accessible to administrator, so the
administrator will login through the security administrator tab. In the following Figure
5.1, we have shown the main page of the Secure Cloud Banking.

![Figure 5.1: Main Page of Secure Cloud Banking System](image.png)

The cloud secure banking web pages are developed in CMS along with supportive
technologies.
Figure 5.2: Cloud Secure Banking Login Page

In the above Figure 5.2, the login web page for the SEPA Admin, login screen will be appearing when Admin click on left side small banner Cloud Secure Banking. After login the Admin will have access to the Secure Cloud Banking.

Figure 5.3: Cloud Banking Admin Portals

The SEPA Secure Cloud Banking page is shown above. Here the Admin will now be able to manage Bank servers, Virtual servers, Bank users and administrators (SEPA Admin and Admin) Administration Portal. Now to bring SEPA Administration Portal in action again a login screen will appear in the figure, it represents second security layer of the system. To get access to resource administrator login again and provide its identity once again.
After verification process is completed at the previous stage, the Admin is now allowed to make change in the system. The Admin is able to add Bank Admin and Assign Bank to that Admin. After that when user clicks on the Add Admin, user will be provided with an API from Identity Management System and information related to user will be stored there. When the user will login again, he will be verified by the Identity Management System Server (IDMS).

After adding the new Bank admin and log in, now the Admin will be able to register the new bank in Secure SEPA Banking System. During the Bank registration, Admin requires specific information for example Bank name, location and Bank Identification Number. After this mandatory information, the bank will be registered.
Figure 5.5: Bank Registration Form

Figure 5.5, shown above, are used for the bank registration. After successful registration, we can check the banks list by clicking the List Banks tab and the Admin will also be able to cancel and go back to the main portal.
Chapter 6

6.1 Future Work

We start this project from scratch, so a lot of work has to be done in the future to secure server and implement new features in the system. In this project, we have not focused on application specific security, but in future we need to implement application level security to secure communication. To ensure end-to-end security in the system, we need encrypted communication between SEPA portal and client application to make it secure channel. In the future, we need to improve all module of SEPA system (clients, servers and portal administration).

To ensure connectivity and communication we need redundancy. In the future we must do work in this area, need some extra services and functionalities in SEPA system. After this, updated structure of the SEPA system will perform well.
References:


[10] Smart Card Clients Master Thesis by Ikram


[12] Secure Administration of SEPA Servers in A Cloud Environment by Hafiz Adnan Ejaz


Appendix A: Code

```html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<%@ page import="java.sql.*" %>
<%@ page import="java.io.*" %>
<html>
<head>
<title>display data from the table using jsp</title>
</head>
<body>
<%
try {
    /* Create string of connection url within specified format with machine
    name, port number and database name. Here machine name id localhost and
    database name is student. */
    String connectionURL = "jdbc:mysql://localhost:3306/iptocountry";

    // declare a connection by using Connection interface
    Connection connection = null;

    /* declare object of Statement interface that is used for executing sql
    statements. */
    Statement statement = null;

    // declare a resultset that uses as a table for output data from tha table.
    ResultSet rs = null;

    // Load JBBC driver "com.mysql.jdbc.Driver"
    Class.forName("com.mysql.jdbc.Driver").newInstance();

    /* Create a connection by using getConnection() method that takes parameters
    of string type connection url, user name and password to connect to database.*/
    connection = DriverManager.getConnection(connectionURL, "root", "");

    /* createStatement() is used for create statement object that is used for
    sending sql statements to the specified database. */
    statement = connection.createStatement();

    //String addr = "37.58.97.207";
    String addr = request.getRemoteHost();

    //String QueryString = "SELECT * FROM ip2nation";
    String QueryString = "SELECT c.country FROM ip2nationcountries c, ip2nation i
    WHERE i.ip < INET_ATON(" + addr + ") AND c.code = i.country ORDER BY i.ip
    DESC LIMIT 0,1";
```
// sql query to retrieve values from the specified table.
rs = statement.executeQuery(QueryString);

String country = "no value";
while (rs.next()) {
    country = rs.getString(1);
}

// close all the connections.
rs.close();
statement.close();
connection.close();
//if country =
out.println(country);
//out.println(addr);
String url = "http://www.yahoo.com";
String url2 = "http://www.google.com";

if (country.equalsIgnoreCase("sweden")) {
    response.sendRedirect(url);
}
else {
    response.sendRedirect(url2);
}

}catch (Exception ex) {
out.println("Unable to connect to database.");
}
%
</body>
</html>