SEPA Clients in A Secure Cloud Banking Environment

Master Thesis in Communication Systems

IKRAM RAHIM

Master’s Degree Project
Stockholm, Sweden 2013

TRITA-ICT-EX-2013:4
Acknowledgements

Thanks God for making successful completion of this Project.

I am very grateful to my Supervisor and Examiner Professor Sead Muftic for providing me opportunity to work at ICT SecLab KTH under his supervision and guidance. His co-operation, guidance, and support throughout the project make this possible. I would like to say thanks to Abdul Ghafoor Abbasi PhD for guiding and giving me his precious time. Here I will mention and will say thanks to Feng Zhang PhD and Hao for providing and assisting me in technical and administrative issues at SecLab.

I would also like to say thanks to my parents and my family members for being so kind and supportive. Thank you so much for supporting and encouraging me during my bad times. How I can forget my friends and Colleagues? I am indebted to all my friends and colleagues who helped and supported me morally during my thesis project. My thanks are due to Hafiz Adnan Ejaz, Salman and Arshad Iqbal for supporting and giving me valuable suggestions around the project.

Finally, I would like to say thanks to KTH for selecting me as a student and providing me the opportunity to study here.
Abstract

Finance and Economics are one of the most important elements in the development of nations.

Dealing with finances and economies banking industry is the solely dominating industry especially during the 20th century. Along with the development of banking industry, information technology was also emerged and started collaboration with this sector. Moreover, banks shifted all their operations over the network; furthermore, networks and telecommunications were enhanced more. They started offering banking services to its clients by using cloud computing (virtualization). After the introduction of Euro by the EU, a project came into existence called Single Euro Payment Area (SEPA). SEPA is an EU project which is an initiative towards the integration and uniform way of payments and bank transfers within the EU region. Our research project is a part of providing web services to clients in a Secure SEPA banking system.

Our research focuses on developing SEPA banking web services for clients. We have developed infrastructure for SEPA banking services. Web clients are going to access the main portal by registering themselves. After registration, a client will create bank account. Bank account will have basic credentials of the client including account number and PIN number. Furthermore, account number and PIN number can be used to check account balance; client can perform transactions and convert the respective currency into Euros. All financial transactions should be dealt in Euros; this is one of the main purposes of our SEPA research project.

In the second part of our research, some activities have been performed with Point of Interaction (POI) devices. POI device is communicating with the banking system through wireless or GPRS protocols; client will use SEPA smart card. Smart card will be swapped in the POI device; device will detect the smart card data and will interact with the SEPA system. Smart card data contain client’s credentials, such as amount in the bank account, 16 digit card number, and cash in, cash out in the account, card expiry date etc. The final portion, detecting the smart card data, is left for future work.
CONTENTS

Chapter-1 Introduction .......................................................................................................................... 5
  1.1 Introduction ........................................................................................................................................ 5
  1.2 Motivation ......................................................................................................................................... 7
  1.3 Problem Statement ......................................................................................................................... 8
  1.4 Background ...................................................................................................................................... 8
  1.5 Objectives ....................................................................................................................................... 9
  1.6 Basic Requirements before starting the Research ........................................................................ 9
  1.7 Research Methodology .................................................................................................................. 10
  1.8 Thesis Outline .................................................................................................................................. 10

Chapter 2 Secure SEPA Banking in Cloud Technology .......................................................................... 12
  2.1 Architecture of Cloud Technology .................................................................................................. 12
  2.2 Cloud Computing Models ................................................................................................................ 13
    2.2.1 Public Clouds .............................................................................................................................. 13
    2.2.2 Private Clouds ............................................................................................................................ 13
    2.2.3 Hybrid Clouds ............................................................................................................................. 13
  2.3 Layers of Cloud Computing ............................................................................................................. 14
    2.3.1 Software as a Service (SaaS) ..................................................................................................... 14
    2.3.2 Platform as a Service (PaaS) ...................................................................................................... 14
    2.3.3 Infrastructure as a Service ........................................................................................................... 15
  2.4 Security Requirements and Concerns in Cloud Banking ................................................................. 15
    2.4.1 Regulatory Policies for Data Protection ...................................................................................... 16
    2.4.2 Data Transfer ............................................................................................................................... 16
    2.4.3 Banks and Private Clouds ........................................................................................................... 16
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4.5 Architecture</td>
<td>16</td>
</tr>
<tr>
<td>2.4.6 Virtual Machine Images</td>
<td>16</td>
</tr>
<tr>
<td>2.4.7 Client side Protection</td>
<td>17</td>
</tr>
<tr>
<td>2.4.8 Hypervisor/ VMM (Virtual Machine Manager) Complexity</td>
<td>17</td>
</tr>
<tr>
<td>Chapter 3 SEPA Secure Cloud Banking Specifications</td>
<td>18</td>
</tr>
<tr>
<td>3.1 Introduction</td>
<td>18</td>
</tr>
<tr>
<td>3.2 Overview of Secure SEPA Banking System</td>
<td>19</td>
</tr>
<tr>
<td>3.3 Smart Cards</td>
<td>19</td>
</tr>
<tr>
<td>3.3.1 Card Standardization</td>
<td>20</td>
</tr>
<tr>
<td>3.4 SEPA Credit Transfer (SCT)</td>
<td>20</td>
</tr>
<tr>
<td>3.5 SEPA Direct Debit (SDD)</td>
<td>21</td>
</tr>
<tr>
<td>3.6 Convergence of Cash Services in SEPA</td>
<td>22</td>
</tr>
<tr>
<td>Chapter 4 Smart Cards Standardization and POI Devices</td>
<td>24</td>
</tr>
<tr>
<td>4.1 Introduction</td>
<td>24</td>
</tr>
<tr>
<td>4.2 Objective of the SEPA Cards Framework (SCF)</td>
<td>24</td>
</tr>
<tr>
<td>4.3 Implementation of Cards and Standards</td>
<td>24</td>
</tr>
<tr>
<td>4.3.1 EPC cards standardization and Services</td>
<td>24</td>
</tr>
<tr>
<td>4.4 Card Services</td>
<td>25</td>
</tr>
<tr>
<td>4.4.1 Cards Initial functions</td>
<td>25</td>
</tr>
<tr>
<td>4.5 POI Device</td>
<td>26</td>
</tr>
<tr>
<td>4.6 Security Requirements</td>
<td>27</td>
</tr>
<tr>
<td>4.6.1 Data Protection Requirements</td>
<td>28</td>
</tr>
<tr>
<td>4.6.2 Card Security Requirements</td>
<td>28</td>
</tr>
<tr>
<td>4.6.3 POI/POS/Terminal Security Requirements</td>
<td>29</td>
</tr>
<tr>
<td>4.7 End-to-End Security Requirements</td>
<td>30</td>
</tr>
</tbody>
</table>
Chapter 5 Design Architecture of SEPA Systems .......................................................... 31

Introduction 5.1 .............................................................................................................. 31

5.2 Architecture and Components .................................................................................. 31

5.2.1 SAFE System ......................................................................................................... 31

5.2.2 SAFE Communication Server ............................................................................... 32

5.2.3 SEPA Bank Server .................................................................................................. 32

5.3.3 Portal Security Administration ........................................................................... 32

5.3.4 Web Server ............................................................................................................. 33

5.3.5 SEPA Customers .................................................................................................... 33

5.3.6 SEPA Web Wallet ................................................................................................ 33

5.3.7 SEPA Mobile Wallet ............................................................................................ 33

5.3.8 SEPA POS/POI Device ........................................................................................ 33

Chapter 6 Implementation and Demo of the System ......................................................... 36

6.1 Content Management System (CMS) ........................................................................ 36

6.2 Eclipse C++ ................................................................................................................ 36

6.3 Init Tools .................................................................................................................... 36

6.4 Apache, MySql .......................................................................................................... 37

6.5 Web Pages and Templates developed in JSP, HTML ............................................... 37

6.6 Demo of the system .................................................................................................. 38

6.7 Conversion ................................................................................................................ 41

6.8 Make File for Project ............................................................................................... 41

Chapter 7 Future Work .................................................................................................. 45

Appendix A: Abbreviations and acronyms ................................................................... 49
List of Figures

Figure 1: Cloud Computing Deployment Models [14] ................................................................. 14
Figure 2: Cloud Infrastructure Layer Model [14] ..................................................................... 15
Figure 3: Secure Cloud Applications – SAFE™ System .............................................................. 32
Figure 4: POI in SAFE System ............................................................................................... 34
Figure 5: SEPA POI smart card reader .................................................................................... 35
Figure 6: Smart cards initial services and basic Functions ....................................................... 26
Figure 7: Application and card standardization ...................................................................... 27
Figure 8: Data Protection Elements ....................................................................................... 28
Figure 9: InitTools.exe ............................................................................................................. 37
Figure 10: Cloud Secure Administration main page ............................................................... 38
Figure 11: Secure Cloud Banking ......................................................................................... 38
Figure 12: Registration Form for Users ............................................................................... 39
Figure 13: Accounts and services ......................................................................................... 39
Figure 14: Account Page ......................................................................................................... 40
Figure 15: Services ................................................................................................................ 40
Figure 16: Transaction Service ............................................................................................... 41
Figure 17: Conversion Service ............................................................................................... 41
Figure 18: Init Tools for POI ................................................................................................. 42
Figure 19: POI Device Information ......................................................................................... 43
Figure 20: POI Device in communication with SAFE System ............................................... 44
CHAPTER 1: INTRODUCTION

1.1 INTRODUCTION

Today is the era of modern science and technology and fast communications. Internet is one of the most important inventions of this era and due to Internet the communications were also made fast. Internet made it possible to perform the fast communications and it has made life easier and comfortable. We can perform our daily routine tasks in a short amount of time and with limited resources. Today everything is related to digital world is possible and can be performed in a short amount of time. During the 90s Internet has experienced a load usage and a large number of users. Since that, everything is shifting on the internet and online banking is one of the latest facilities which have been recently introduced. Secure SEPA (Single Euro Payment Area) banking system is one of the areas which are going to be introduced in the near future.

SEPA stands for Single Euro Payment Area, an EU initiative in banking area which is related to payments and transfer of money within the EU region along with Switzerland and Macau. SEPA idea came into existence by the EU governments in the Lisbon Treaty in March 2000. The stakeholders in SEPA including EU governments, and European Central Bank (ECB) are going to introduce the integration of the Euro in the area of payments. In 1958 after the introduction of the European Economic Community (ECC), different events moved towards an integrated European financial market. In the first process, they introduce Euro in 1999. It was the first step towards the integration of the European Financial Market. SEPA project was the second project towards the integration of finical markets. SEPA gives advantages to customers and merchants to perform any financial non-cash Euro payment into Euro payment within the geographical locations of Euro by using SEPA account. SEPA include only single currency, credit transfer, and direct debit and credit card payments [3].

By the end of this research project, it will facilitate the credit transfer, debt schemes, payment schemes and it will convert a Euro into a fully operational national currency within its geographical locations. There will be a SEPA card used by the customers, which will enable the customer to perform payments, as well as e-transactions. SEPA accounts will be used within the certain geographical location where Euro is applicable. In SEPA accounts, national currencies should be dealt with Euros [1].

By introducing SEPA business and customers within the SEPA region users, will be facilitated with the SEPA debit and credit cards. They can perform many kinds of services like payment, transactions, and conversion of respective currencies to Euro. There are many advantages of SEPA system, one of them is that merchants and customers will get many advantages from one single Euro market. Especially in case of businesspersons and companies where they have many setups and multiple branches within the Euro region will be freed from keeping different
accounts in different regions. The entire SEPA standard will be the same within the SEPA region. By introducing the same common practices in terms of SEPA, payments will create more opportunities for single payment solutions without any hurdle. SEPA will bring more positive and competitive environment, mostly in banking and other industries.
1.2 MOTIVATION

The main motivation for doing this research project is to do research in such a project where there is uniform and homogenous banking system. All financial activities and business matters shall be dealt in Euro. Before this project, many countries have their own banking policies and regulations. Although after the project there will still exist their banking systems and currencies, but ultimately they will have a uniform banking system and procedure. It will create a competitive environment in banking industry and EU will come more together to each other.

The other reason behind this development is that the final product will be introduced in the form of secure banking system. The world has turned into a global village due to tremendous development in the field of technology. Everything has turned to the Internet and now people are using mobile online banking. This project will be finally deployed using cloud technology. Cloud technology has been introduced recently, so it is also a motivation towards this project.

In banking, system there will be some smart card devices which will connect to the SEPA bank. SEPA is currently working and soon will introduce the POI devices for smart cards as well as standards for smart cards and POI devices. Keeping POI, smart cards standards, and their security is also a motivation to work in this project.
1.3 Problem Statement

The problem statement is to facilitate to the customers and accelerate different web services that go on to a sale point (SP) and use their bank cards for payment. They will do a secure payment via the Visa card machine. How can Visa POI be used with SEPA payment which is different from Visa? The client will use smart cards to perform transactions.

In this thesis project, we will study current aspects and elements included in the existing SEPA banking system and will do some research and will develop SEPA web services for Secure SEPA banking system. Clients will use secure SEPA banking web services, such as payment, transaction, balance check, and currency conversion.

In another part of this project, we have researched POI devices which will be used to interact with the Secure SEPA banking smart cards. Users will swap the smart cards and, after reading, all the details of smart cards POI device will interact with banking server and will transfer the payment. Smart card reading by POI device was left for future work.

1.4 Background

Before the introduction of SEPA banking system, countries within the EU, Euro is in use for business deals, regular financial transactions, and payments. Countries within the Euro zone were using the Euro, excluding some Scandinavian countries, as well as outside of the Scandinavian region. Besides using Euro, every country has its own banking system, rules, and policies. They had their own policies rules and regulations. Due to different banking systems and policies, it was hard for businesspersons and general customers to establish business or other financial setup. Even transferring amount from one country to another country was slow and with high cost. ECB and some of its organizations came to a conclusion that there should be a uniform banking system within the EU region including Switzerland, Macau, and few other countries. After the feasibility study, meetings, and hard work they established SEPA systems.

Single Euro Payment Area (SEPA) is an initiative step towards the process of integration of a Euro into a single, uniform, and homogenous banking system. Within SEPA banking system, customers and merchants will be facilitated by performing payments, low cost effective and fast transactions within the Euro region. Payment and transactions will be performed very easily and securely. After the completion of SEPA, there will be no difference between national and cross-border Euro payments [4].

The SEPA project is supported by the European Commission and European Central Bank (ECB). Once the SEPA is established, customers and merchants will be able to make fast and secure money transfers by using SEPA bank debit/credit cards within the Euro region. SEPA will bring competitive environment in the banking industry particularly within the Euro region.
1.5 Objectives

The main objective of the SEPA project is that it is an initiative towards the integration of SEPA financial market. In countries where all users belong to Euro region they will easily perform transaction and payments. During the initial phase of the project, we will do research on SEPA aims and how is our role within the SEPA banking project. We are going to provide services to SEPA bank users through online banking transactions as well as through SEPA debit and credit cards. Users will have bank account and SEPA debit and credit card which they will use for online transactions, payment as well can swap in Point of Sale (POS)/Point of Interaction (POI) devices. Information can be retrieved from the card and will be forwarded to the bank server. After verification, the services can be performed. The main objectives are:

- Client can register, create, and update account using SEPA bank.
- Client will use SEPA bank smart cards to perform transactions.
- Client will online check his/her bank account status.
- SEPA client/user will be able to pay during travel, outdoor activities, shopping, hotel, or any other spot within the Euro zone by using his/her SEPA debit/credit smart card by POI device.

After successful completion of this thesis project we will be able to get deliverables in the form of web services for SEPA users whom can use the system for online payments, as well as on the cards payments using POS/POI devices. All SEPA users will be able to check their balances in bank accounts, convert their respective currencies into Euros, and transfer to another account.

1.6 Basic Requirements before Starting the Research

The main requirements before starting the project are to know what is Single Euro Payment Area (SEPA)? What is its role in banking industry within the EU? What effects will bring it in the life of general customers as well as merchants by introducing this scheme in terms of banking, as well as politically in the region. Moreover, as Secure SEPA, banking system is going to be a part of digital and IT world, all services will be implemented in a cloud-based technology. These services will be available online to their respective clients. Therefore keeping all these points in mind, we have to know the implementation of this scheme, its security aspects, and implementation in a cloud-based technology. We have to make the project viable, applicable, and more than secure to get trust of clients and organizations that are going to be a part of the SEPA project in near future. We also have to look its security implementations, in this regard. Some standards have been approved by the EPC, EU, and SEPA, and some are in the process. Standards have been finalized in terms of the devices like POI/POS devices, SEPA direct debit (SDD) and SEPA credit transfers (SCT).
1.7 Research Methodology

Research methodology is the way of finding out the hidden facts and way of searching the knowledge. Some writers define research as a “scientific and systematic way of specific information on a specific topic”. It is a kind of discovering, enhancing, and evolving the existing structure of facts and knowledge. While some authors think that research is a kind of movement, movement of and undiscovered, unidentified facts and figures to known and defined facts. Researchers and scientists have defined many ways of finding out the hidden areas of research; one of them is Design Science or Design & Development Research. We also adopted this method during our research [8] [9].

The basic purpose and motivation of adopting this approach to of research is that, it covers the overall process. It’s a kind of method which covers all the areas around it. It is different from conventional ways e.g. conducting surveys and interviews, co-relational analysis and other ways of finding facts. There is also another reason for choosing the development and research method; it turns the complex research, complicated topics in the form of education in worldwide.

There are many other research methodologies and approaches, they are given below.

- Design Studies or Design Experiment or Design Research
- Development Research
- Formative Research or Evaluation
- Action Research
- Engineering Research [9].

1.8 Thesis Outline

This thesis project is based on secure cloud banking, in which we have developed web services for SEPA users as well as smart card users. Our report consists of a general introduction about the research project, background of the SEPA secure banking and its integration, motivation, problem statement, goals and objectives.

Chapter 1 gives a brief introduction of the SEPA project. What is SEPA Secure Cloud banking? Chapter 2 discusses about Secure Cloud banking: its environment, about Clouds and its different deployed models. Chapter 3 describes SEPA systems, overview of SEPA banking standards, specification, and requirements. It discusses about the cards standards, SEPA direct debit, and SEPA Credit transfers. Chapter 4 gives explanation SEPA cards, POS/POI devices, general security, and specific requirements of smart cards and POI devices. Chapter 5 explains design architecture of our SEPA system, its flow and communications with other systems for example
SAFE system, SEPA web portal etc. Chapter 6 describes about the implementation of our system and has a portion about the demonstration of our system. Chapter 7 discusses future work.

Some useful material which are used in the thesis, but is outside the main flow of the thesis, will be kept in appendixes.
**CHAPTER 2: SECURE SEPA BANKING IN A CLOUD TECHNOLOGY**

Cloud computing is a new term introduced recently in the field of computer technology. Basically cloud computing is the use of new resources including both hardware and software, which provide fast services over the network/Internet. According to Andrew Moore cloud computing is the third revaluation of IT. Cloud computing is a concept or a model in computing where capacity for storage or networking can be acquired according by the demand of the user and pay according to the services which are issued. In other terms, cloud computing is an outsourcing of IT functions over the network which are provided remotely rather than using a physical IT infrastructure. In a cloud computing user can be an individual or from a small company to a large multinational organization. Due to this new model, services are going to be introduced to the users by using less capital, without physical storage capacity. It will increase computing efficiency and will be beneficial to reduce risk of operation in any kind of organization [10] [11].

Here we will discuss moving of banking industry into cloud environment. We all know, some organizations will hesitate to convert to cloud environment. However, banking industry is dealing with sensitive issues especially with the public capital. Banking industry will make sure and will think before they should shift to a cloud or not, and they will have to ensure and address all security issues concerned with the cloud technology. The most important element is to avoid monetary scams data privacy and security. Before we may go into more details, we will go through the structure and different flavors of cloud technology.

### 2.1 ARCHITECTURE OF CLOUD TECHNOLOGY

According to the earlier cloud models, cloud computing runs on the bases of three fundamental models. They are:

- **Software-as-a-Service (SaaS)**
- **Platform-as-a-Service (PaaS)**
- **Infrastructure-as-a-Service (IaaS)**

The above mentioned three approaches are based on virtualization. During the last few years, a lot of development and improvement have been done in cloud technology virtual machines. Due to virtualization more flexibility, enhances a dynamic data centers and provides more available resources in terms of available servers, according the needs of the process. Virtual machines are very efficient in terms of scalability and have ability to deploy applications very
rapidly. Standard deployments of objects and virtual machines are the best and standard way of implementing cloud computing [12].

**2.2 CLOUD COMPUTING MODELS**
Based on cloud computing concept there are several infrastructure models when organizations want to deploy their services toward cloud technology. There are public, as well as private clouds, each model have their own advantages.

**2.2.1 PUBLIC CLOUDS**
With cloud computing, organizations choose which model they want to deploy for their services and which is suitable for both organization, as well as its clients. Public clouds are run by the third party; they mix the applications used by other clients on cloud servers, storage systems, and networks. The model is usually separated from the premises of the users. They have been provided a temporary extension to enterprise infrastructure. Public cloud is designed and implemented by keeping some elements in mind like security, data locality, performance and the existing services are both accessible to the cloud architects and end users too. Public clouds give services to many clients while they are deployed at a point where they collaborate with its clients.

**2.2.2 PRIVATE CLOUDS**
Private clouds, as it is assumed from their name, are built and associated to a client, where the client has most access and control of it. The client is handling its data availability, security, data usage and other applications deployment. This model provides companies high level of control over the cloud resources, and companies own the infrastructure as well as control.

**2.2.3 HYBRID CLOUDS**
Hybrid cloud is a collaboration of both public and private clouds, which are helpful in a collaborative and on demand services model. Hybrid cloud can be used to share the workload and can perform periodic tasks. Those tasks are then easily deployable on public clouds; this process is called “Surge Computing”. Hybrid cloud may be more efficient and successful if a large amount of data can be shifted into a public cloud, while processing is very small in terms of size. This could distributes the load over the cloud. Clouds deployment model is shown in Figure 1 [13].
2.3 Layers of Cloud Computing

In this section we will discuss architectural layers of the cloud computing. Cloud service providers have categorized those layers in three groups: Software-as-a-Service, Platform-as-a-Service and Infrastructure-as-a-Service. These various layers and categories are described as the following.

2.3.1 Software-as-a-Service (SaaS)

SaaS cloud layer provides services on demand and complete application according to the client's requirements. This runs over the cloud and provides services from a single user up to the whole organization. Google apps, including word processors and email services, are the examples of the SaaS layer.

2.3.2 Platform-as-a-Service (PaaS)

PaaS is basically used for building higher level services. For building these services, it encapsulates Software-as-a-Service. It services are based on the requirements for consumer or producer. There are two options working and developing infrastructure with PaaS:

• If a platform is created by collaboration and integration of Operating System and application software and middle is offered to a customer.
- An encapsulated service is developed and offered for service and presented through APIs. Customer using APIs to interact with that service. Virtual applications are offered through this service.

Google Applications Engines are examples of PaaS.

### 2.3.3 Infrastructure-as-a-Service (IaaS)

IaaS provides facility of storage, computing capabilities and standardized services over the network. All servers, routers, switches, and other services, which are used in any cloud model, are offered by the IaaS. It provides high-on demand infrastructure, as well as load balancing and sharing services to the cloud environment [13].

![Cloud Infrastructure Layer Model](image)

**Figure 2: Cloud Infrastructure Layer Model [14]**

### 2.4 Security Requirements and Concerns in Cloud Banking

As we are going to introduce banking system and then provide services to web clients using cloud environment, so there are some security requirements and concerns by adopting this technology. Banks have sensitive data, they have always concern about their data, and they need specific requirements. Those concerns, guidelines, and requirements are discussed here.
2.4.1 **REGULATORY POLICIES FOR DATA PROTECTION**
Inadequate Policies and Practices are not complete and need more regulations and laws in this regard. Within the EU, banks are required to act over Markets in Financial Instruments Directive (MiFID). The main purpose of MiFID is to introduce competitive market and their client protection across the Member States.

2.4.2 **DATA TRANSFER**
We discussed earlier that public clouds can be controlled and run from anywhere in the world. Organizations are shifting to cloud environments, so for capacity demand there are many data centers established in different locations. Due to these options, when banks are transferring their data to clouds, they need high level of data transfer protection, as well as to meet requirements of data protection law.

2.4.3 **Banks and Private Clouds**
Banks are always restricted to perform business critical functions in the public clouds and they may restrict this towards adopting private clouds. However, at the time of establishing public clouds, banks should be obliged to adopt and follow a step towards virtualization. In this case, they can reduce hardware, software, energy, as well as infrastructure cost. In addition, they should keep an eye and some other elements, for example securities, reliability, inter-compatibility issues must be considered [15].

2.4.5 **ARCHITECTURE**
For any specific cloud model, which is going to be used for services, providing its software and hardware are different from each other. It also depends on the model of the cloud and all specifications, for example scalability, reliability, resource pooling, and other logics, which are involved in building a model, are decided by cloud architects. In cloud technology virtual machines are the main unit for deployment of the IaaS model. Some cloud providers also use computation abstractions in virtual machines for the use of services in other cloud based models [16].

2.4.6 **VIRTUAL MACHINE IMAGES**
IaaS and virtual machine providers keep repositories of the virtual machine images. Each machine having its configurations of different services, installed software, and configured applications to boot the machine. Although it is a very common way of sharing virtual images of the machines, but the provider will have to configure it very carefully, to avoid technical faults and bugs. Because an attacker can attack the image of the virtual machine and can change or hack the key information, or the attacker can put some viruses and can attack the consumers
data in the cloud. Therefore, researchers always encourage the organizations for the implementation of formal image management process. In this way they can manage the creation, running, storage and use of virtual images very well [16].

2.4.7 Client Side Protection
Cloud computing is safe until we can avoid both client and server side attacks from the hackers attacks. Web browsers and growing social media trends are the most common ways of attacking the either side. Second important element is to establish and maintain both the logical and physical security in embedded technology and the most common technology is the introduction of smart phones. Due to portability sometime the client can lose physical control, the attackers can overcome the used and unused built in security mechanisms, as cloud applications are configured and served in the form of built in applications or installed plug-ins. So smart phones are used with limited set of functions in a cloud and they can be kept as fixed appliances. Due to this security architecture used in cloud computing, organizations are required to think about the existing architecture and work for its enhancements. Security measures and trainings in organizations, as well as on individual basis, will also be beneficial for data protection [16].

2.4.8 Hypervisor/ VMM (Virtual Machine Manager) Complexity
VMM is very important software in virtualization which is responsible for creating and running virtual machines. VMM is responsible for running different virtual machines as it is stated that each cloud model, like PaaS, SaaS or IaaS can be run and handled individually. Therefore, all these virtual images, cloud applications run individually and simultaneously on a single computer. It will look simpler, but the modern VMM are built more complex. Therefore, it is very important for a cloud provider to know how about the security risks and measures before the implementation of virtualization [16].
CHAPTER 3: SEPA SECURE CLOUD BANKING SPECIFICATIONS

3.1 INTRODUCTION
We have already discussed earlier about our research and SEPA. In this chapter we will give complete details about SEPA and SEPA secure banking, its goals, aims and about SEPA vision. SEPA secure banking is an initiative and step towards the integration of payments, and transfer of money in Euro zone came under the consideration by the European Union Commission (EU). Its aim is to enhance and improve bank payments and turn it into a single and identical process in the region where Euro is applicable. SEPA integration process started in 2002 after the introduction of Euro currency. This work started by the EU governments, European Central Bank (ECB), and some other organizations working under the EU Commission. Today there are 27 EU member countries as well as some other countries, which do not belong to EU are working under the SEPA governing body.

EU and other governing bodies as the stakeholders have set certain milestones for the SEPA project. The main goal is to improve payment transfers within the EU borders and make them efficient, as well as faster. All domestic banking processes should be integrated into a single and easy processed solution. By introducing SEPA, integration idea will reduce the cost of payment and moving the capital within the EU territory. SEPA is looking forward for two major processes. One is Pan-European payment instruments, which will process debit and credit cards. The second by the end of 2010, the national payment methods will be much developed to increase efficiency and integration of economies. EPC (European Payment Council) has already defined the the limits and regulation for transferring the payment via debit/credit cards. We will further discuss about SEPA debit and credit card transfers and its functions [3] [4].

One of the main objectives of SEPA is also to decrease the use of cash and to introduce more use of electronic payments and money. In case of electronic money transfer, they will overcome money laundering cases. It is also discussed that besides one payment system, it should be ensure that payments should be transferred securely. The payment process shall be executed and conducted electronically and secure. Customers and merchants will use IBAN (International Bank Account Number) and SWIFT code for transferring money. In SEPA scheme there will be only one bank account, all the payments will be performed via debit/credit cards [5].
3.2 Overview of Secure SEPA Banking System

We have discussed about Secure SEPA banking system. In this section we will discuss in detailed what actually SEPA banking system consists of. Moreover, how it will work and how the standards will be in SEPA kept by the governing bodies?

There are many stakeholders involved in this process, so all the processes should keep in mind to develop this SEPA banking system. In SEPA, the main focus is banking and finance area. There are payment areas and processes which are discussed and implemented. There are three main areas which will be focused in the SEPA banking system. These are introduced by the approval of EPC (European Payment Council). One is the infrastructure for the payment and the remaining two are payment methods [3]. They are as follows:

- Smart Cards
- SEPA credit transfers
- SEPA direct debits
- SEPA credit payments

The first two mentioned above will be discussed more in details. Moreover, SEPA system will also introduce additional financial services to facilitate customers and merchants [3]. They are:

- Faster settlement for payments
- Mapping Bank Identifier Code (BIC)
- International Bank Account Number (IBAN)

3.3 Smart Cards

We have discussed SEPA schemes which they are going to introduce to their customers for payment transfers. Special cards under the SEPA regulations are also under development. We know from SEPA annual progress reports that the desired progress is still not achieved and they are trying to speed up the process, but the competitive card market capability in SEPA still exists. Euro system is keeping an eye on its progress and its implications in SEPA scheme. Euro system is also keeping its standard in mind according to the market as well keeping easiness in terms of both transfers, as well as benefits of SEPA card users [6].

Furthermore, SEPA is also taking guidance in terms of multilateral interchange fees (MIFs) from the European Commission in regulatory forms and commitments made by the MasterCard and Visa Europe. SEPA is trying to remove all the hurdles step by step which they are facing in terms of smart cards and its standards. They are planning by the end of 2013 to issue SEPA wide licensing. It means that card and license issuance will not be only limited to specific countries,
but will be issued by any SEPA region country. The security concerns will be addressed and solved on the basis of mutual understanding and agreements between EPC and other members [6].

According to the experts, a new card scheme is capable to bring economic and political benefits to the region. By introducing new card scheme, the market will become more competitive; other stakeholders will also come out and will invest in this field. The providers will try to make their schemes more efficient, low level fee and other benefits. Moreover, the action over the cards scheme for SEPA will ultimately reduce the costs of cash handling for banks and other clients [6].

### 3.3.1 Card Standardization

We discussed about the card scheme in the Euro system and SEPA, so it is very important to define smart cards standards and their implementation in SEPA. Euro system is making it very clearly to keep one standard over the distribution of the standard of the cards within the region. Therefore, EPC established Card Stakeholders Group (CSG) in October, 2009. There are five main stakeholders in CSG group: banks, card schemes, processors, manufacturers of cards and terminals, and retailers. CSG is responsible for development and maintenance of uniform standardization and security requirements for card services.

Euro system is expecting complete clarity from the EPC in all standards which are currently in use and those standard which will be used in the near future for end-to-end transactions using POS (Point of Sale) and ATMs as a medium. The standardization where the CSG is responsible to keep the same standards in different domains is card-to-terminal, terminal-to-acquirer, acquirer-to-issuer, certification, and type of approval. There are various initiators in different domains and standards, for example CIR TWG, EPAS, Berlin Group and ISO. Developments and its implementations are in progress, but the main focus is to bring them and apply them in a uniform way.

Now we will talk about SEPA security implementation in a certificates framework CAS (Common Approval Scheme) is taking care of this domain. Certificate management and SEPA security framework have been approved by the EPC. Although management has been approved some concrete discussion are still going on. Euro system is waiting for the output expected from EPC and CAS members. Consequently, Euro system and all the stakeholders are waiting for the final uniform standardization in terms of cards and other devices, which are going to be the part of this scheme [6].

### 3.4 SEPA Credit Transfer (SCT)

SEPA Credit Transfer (SCT) was first introduced in January 2008. SCT (SEPA Credit Transfer) was very appreciated and welcomed in the project which was developed by the European banking industry. SEPA has also ensured more efficient and beneficial services by using the SCT.
deployment of SEPA, the SCT will become a credit transfer tool within the Euro system. Total of 95 percentage of banks within the EU are adopting process of SCT for the credit transfer [6].

Euro system is also keeping an eye on the progress and use of SCT scheme. It is noticed that since the introduction of the SCT, its usage has been increased and total ratio was raised up to 9.3% in August 2010. The indicator also mentioned national level in each country on the basis of national legacy products and credit transfer. Earlier in 2008 and in 2009 SEPA migration rate to SCT was slower.

3.5 SEPA Direct Debit (SDD)

SEPA introduced its direct debit scheme in November 2009. Euro system and European Commission has introduced three schemes under the SDD:

- SEPA core direct debit scheme
- SEPA business-to-business direct debit
- SEPA fixed amount direct debit scheme

The first two are related to electronic transfer, while the last one is under discussion by EPC. Like SCT Euro, system is also keeping an eye on the migration of domestic direct debit transfers to SDD. They use the SDD monitoring indicator based as in SCT they measured it by the credit transfer by percentage share of all the credit transfers. All the calculations and measurements are based on the basis of aggregated data which is acquired from different systems and infrastructures based in the EU Commission. During the collection of data and statistics, they took data from all countries within the Euro zone. They have defined certain rules, regulations, and special parameters to get to the conclusions. [6] [7].

Design of SDD is a long term and time consuming process. The reason why it takes so much time that it must is solve different issues involved in it. As we discussed earlier, few of the issues are multilateral interchange fees (MIFs) and the existing card issuing companies, as well as security concerns during the transfer of payments. Currently the EU has resolved MIF for SSD by using Regulation No 924/2009 on cross border payments. The EU commission and ECB have issued joint statement on the future of SDD business model. This model is based on the regulations of cross border payments which only work on temporarily charging model which will be valid until November 1, 2012[6].

Furthermore, the paper-based mandates, SDD is planning to launch mandates generated by using electronic channels, which are called e-mandates (electronic-mandates). These e-mandates facilitate online banking services. When any debtor wants to use it, he/she can access those services by giving his/her credentials. E-mandates facility is especially suitable for large scale transfers, especially for businesspersons and merchants. EPC has introduced first e-
mandate to banks to offer the service. Portuguese banks were the first to introduce it in banking industry. E-mandate is an optional service. However, EPC always encourages the banking industry to offer this facility. Ultimately it will increase the acceptance of the SDD in the SEPA region and customers will use more e-payment schemes within SEPA region [6].

If we compare the SDD progress and adoption with the SCT, its adoption and eagerness was slow by the banks. It was due to the fact that some countries tried to postpone the SDD launching by the due date. If the national direct debt schemes are successful, it directly effects design of the SDD, which will ensure a new way of payment method. Its success will be sure if the new method and its tools are user friendly with use, as well as customer satisfaction, in terms of security and confidentiality, price, services, etc [6].

### 3.6 Convergence of Cash Services in SEPA

In July 2010 through a regulation the EC decided about the professional cross-border transportation of Euro by road within the member states. The procedural steps were included in the conversion of cash were offered and discussed by the Euro area. This basic and free of charge service is in process and will be part of the SEPA.

As we discussed earlier, after introducing the Euro, Single Euro Cash Area (SECA) was turned into a reality for the European consumers. After that NCB, started thinking to provide services of cash convergence to their major clients and customers. In February 2007, all the stakeholders in the Euro system ensured a roadmap for the further convergence of NCB cash services [6].

In July 2010, another proposal was suggested about the cross border transportation of cash. Basically, it was an EU regulation for the professional cross border of the euro cash by road within the Euro region. They introduced a common rule within the whole region; all the proposals and suggestions will be discussed in the EU Parliament, as well as in the EU Council for further process. Meanwhile they have finalized two steps in this process. Those two steps are:

1. **Electronic data exchange with clients for cash payment and withdrawal**
   - Euro system has introduced a common method in which professional clients will communicate electronically, that will ensure e-payment and withdrawal of money across the borders. A common platform was introduced which is called Data Exchange for Cash Services (DECS). It is working on two main formats which already exist in the Euro system: one is called GS1 and the second is CashSSP. All the stakeholders along with NCB are expecting its implementation and connection with DESC by the end of 2010 [6].

2. **The second step which is already working is introducing common and free-of-charge services.**
   - Euro system is now taking step toward a common free-of-charge services.
cash services for their clients. They are comparing and trying to satisfy the concerns about the security issues raised by the EPC and European Security Transport Association (ESTA). After comparison with the existing packages and features, they will try to sort out all the constraints and form a unique and one common system. After careful consideration by the authorities, they will introduce a common approach in the Euro system [6].
CHAPTER 4: SMART CARDS STANDARDIZATION AND POI DEVICES

4.1 INTRODUCTION
SEPA Card standardization and framework, defined by SEPA, will be used in the future when the SEPA project has to be completed. The purpose of these standards is to set up an initial foundation for the cards where they can be updated from time to time and will be deployable easily in the SEPA region. These standards can be used for cash withdrawal, as well as for payment within the region. Keeping standardization is to address all the conflicts and solve all the challenges in the cards schemes which are addressable by issuers, as well as by users. Therefore, before deployment of the card schemes, all stakeholders as well as users, will agree on one standard to avoid any sort of conflict. The European Payment Council (EPC) has taken steps of dialogues among the stakeholders, to identify the main principles and possible solutions to implement all the standards across the EU. To achieve that goal, they established a group called Card Stakeholders Group (CSG) [24].

4.2 OBJECTIVE OF THE SEPA CARDS FRAMEWORK (SCF)
The main purpose and objective of the SCF is to build principles and standards to meet different market requirements and create competitive market. European policy makers acknowledged that by adopting the card standardization. EPC is working for SEPA cards standard in general. They are working on card payments and cash withdrawal services. They have involved different stakeholders, like SCF complaint card schemes, issuers, acquirers, processors, vendors, etc. SEPA Cards Standardization Framework aims are to bring the same standards and security requirements, as well as to introduce the SCF SEPA Cards Standards [24].

4.3 IMPLEMENTATION OF CARDS AND STANDARDS
As we discussed earlier about the cards and standards, all these standards are defined and will be implemented by the approval and mutual discussions by all the stakeholders. They will create a competitive environment among the stakeholders and they will try to improve its standards.

4.3.1 EPC CARDS STANDARDIZATION AND SERVICES
SCF and EPC define high priority of card standardization within the SEPA. They have developed it according the requirements and needs of the stakeholders. In this section, we will discuss about the cards and their functions. Financial transaction is one of the functions which are offered by the SEPA smart cards; all these are related to cardholders, also discussed in the EPC document version 5.5. When we use the card services, there are several stakeholders involved in it. They are:
• Card Holder (Owner of the card who pays the money)
• Issuer of the card (Origination who provide the card service)
• Payee (Card acceptor)
• Acquirer (“Payment Service Provider” of the card acceptor)

The payer and the payee interact with each other through a particular card technology and machine with Card Holder Verification and Card Authentication Methods. One of the technologies used for card interaction is Point of Interaction (POI) sometimes called Terminals used by the cards and cards acceptors [24].

4.4 CARD SERVICES

Smart Cards have chips, they are used of keeping information and also to connect to system for payment. There are some many card acceptance technologies in card services. For example, Europay, Master Card, and Visa(EMV) [25].

• There is only Automatic Application Selection when we use EMV Entry Point.
• There is no offline PIN for Cardholder Verification in EMV.
• For one-tap, contactless process completion is performed without card contact [24].

Some cards are used without having chip.

• Card based Language selection is not available.
• Application selection is unavailable.
• Card Authentication is not activated in these cards.
• Cardholder Verification cannot use the offline PIN.
• Authorization service has not been included in cards without chips.
• Offline magnetic stripe transactions are performed without authorization [24].

4.4.1 INITIAL CARD FUNCTIONS

There are some initial functions with smart cards. Some of them are Manual Language selection, which is optional. Before initiating a transaction Manual Language selection should be available for selection. In case of selecting Manual Language option, it is directed that selected language shall be used for the whole transaction, but Card Based Language selection will be disabled. In
case of not supporting the Language Selection Language Selection, shall be utilized only in chip-based transactions. It depends upon the selection and the priority when we choose an option, also the card retrieves information from Payment Selection Environment (PSE). Card-based Language Selection, the same as Application selection, is only available for chip-based cards transactions, while Technology Selection and Card Data Retrieval is only available in case of card present [24].

Smart card services functions, and service and language selection criterion are shown in Figure 3.

<table>
<thead>
<tr>
<th>SEPA Smart Cards Services and their Basic Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Manual Language Selection</strong></td>
</tr>
<tr>
<td>A) Manual Language Selection</td>
</tr>
<tr>
<td><strong>Technology Selection</strong></td>
</tr>
<tr>
<td>Technology Selection</td>
</tr>
<tr>
<td><strong>Application Selection</strong></td>
</tr>
<tr>
<td>A) Manual Application Selection</td>
</tr>
<tr>
<td>B) Automatic Application Selection</td>
</tr>
<tr>
<td><strong>Card Based Language Selection</strong></td>
</tr>
<tr>
<td>B) Card Based Language Selection</td>
</tr>
<tr>
<td><strong>Card Data Retrieval</strong></td>
</tr>
<tr>
<td>A) Read card data from physical card</td>
</tr>
</tbody>
</table>

*Figure 3: SEPA Smart Cards initial Services and basic Functions*

**4.5 POI Device**

POI is a device which is embedded with a software application used for smart card reading. The smart card holder can perform transactions using POI or can perform transactions by using bank web services. Application profile decides processing parameters for POI Application; those parameters play an important role in performing transactions. If there are card holders
transactions Application Profile, its function is based on Card Application Identifier on the card service and acceptance technology. If the transactions are performed remotely, then Application Profile is based on the product selection by the card holder. Figure 4 given below shows the relationship between POI Application, Application Profiles Card Services and card Functions.

![Diagram](image)

**Figure 4: Application and Card Standardization**

Note: Functions related to and supported by POI application

Services are those implemented and supported by the POI application

POI Parameters define POI Applications which are used for Card Services. Card Services Parameters are used in configuring for card services and different acceptance technologies. In acceptance technologies POI devices and card types are more prominent. Application Profile parameters define application profile, e.g. how to use profile for card services Moreover, it defines the limit and level for the Card Service [24].

### 4.6 Security Requirements

In this section, we are going to discuss security requirements for POI and for different card systems. Defining and fixing security requirements are crucial for all stakeholders involved in the cards schemes, as well for POI devices. Those requirements are also matching the SEPA requirements and can match with the SEPA systems. All credit and payments institutions within the SEPA are obliged under the SEPA regulations to implement and act upon on the security
requirements, which are suggested for them, so that the customer should not be affected by scam, frauds, and other negative activities.

4.6.1 DATA PROTECTION REQUIREMENTS

Data protection is the most important factor in any organization, especially in the banking and finance sector. Keeping it in mind Payment Card Industry Data Security Standard (PCI DSS) has introduced certain baseline requirements to protect account data. SEPA has recommended that establishing security requirements and keeping standards in different environments has to be set by different card schemes. CSG will be responsible for bringing the uniformity within the schemes and security requirements. PCI DSS has set certain elements for data protection. They are shown in Figure 5 [24].

<table>
<thead>
<tr>
<th>Account Data</th>
<th>Element Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Holder Data</td>
<td>Primary Account Number (PAN)</td>
</tr>
<tr>
<td></td>
<td>Card Holder Name</td>
</tr>
<tr>
<td></td>
<td>Service Code</td>
</tr>
<tr>
<td></td>
<td>Expiration Date</td>
</tr>
<tr>
<td>Sensitive Authentication Data</td>
<td>Full Magnetic Stripe Data</td>
</tr>
<tr>
<td></td>
<td>CAV2/CVC2/CVV2/CID</td>
</tr>
<tr>
<td></td>
<td>PIN/PIN Block</td>
</tr>
</tbody>
</table>

Figure 5: Data Protection Elements

4.6.2 CARD SECURITY REQUIREMENTS

Smart Cards always play an important role in financial online transactions, as well as for Point of Sale locations. Therefore, SEPA has recommended evaluation and security requirements for smart cards to ensure the security and safe transactions. As we discussed payment, application mainly consists of transaction schemes defined by card schemes. Here it is assumed that all smart cards have EMV capabilities. Some of the capabilities are the following:

- Selection of Application
- Initiating Application
- Offline communication with Terminal
• Data Authentication(Offline), both static as well as dynamic, if the card supports dynamic RSA computation

• Online Communication, as well as Authentication, with the issuer

• Verifying the cardholder by using PIN comparison

• Analysis of Card Action (Internal risk management)

• Issuing Transaction Certification

• Scripting processing means updating Payment Application parameters and software

• Internal State Management to ensure that the above steps and processes have done successfully.

During the initial introduction of smart cards, it is supposed and recommended by the SEPA that all cards have EMV support. EMV is used a baseline for SEPA cards [24].

4.6.3 POI/POS/Terminal Security Requirements
We have discussed earlier about POI devices. SEPA and other stakeholders involved in this project have assured the POI security. All these stakeholders are in regular process of discussing the security issues as well as improving the security standards time by time. They have taken care of each and everything, from manufacturing of the device up to the customer. During the manufacturing, the manufacturer has taken care of:

4.6.3.1 Core Physical Security Requirements
Secure components for unattended devices contain an anti-removal, in order to protect unauthorized installation and removal. The mechanism is defined as the potential if some unauthorized, unidentified person trying to hack the device.

4.6.3.2 POS Terminal Integration
Approval of POS integration is based on the entering the PIN by the user and acceptance of PIN by the device. In POI, device PIN acceptance is secured both logically and physically. However, it can approve and can allow re-using the previous components such as card readers, display, keypads, and secure processors. This module is cost effective and has the capability of security management requirements for integrated devices.

POI application must enforce the communication between the device operating system and cardholder. If the commands and impacting the correspondence between the operating state of the device and the messages, the commands enabling the data entry must be authenticated.
4.7 END-TO-END SECURITY REQUIREMENTS

In this section, the stakeholders defined End-to-End security requirements are listed. SEPA and EPC have just defined this for information and need contributions from the stakeholders and other parties. These requirements shall be considered for different domains, End-to-End security requirements are the following [26].

- Encryption of Device (Both software and hardware)
- Application on the device
- Merchant encryption environment
- Generic applying encryption and decryption operations
- Decryption environment
- Key management
- Host Processing
- MAC’ing and Signature
CHAPTER 5: SECURITY ARCHITECTURE OF THE SEPA SYSTEMS

5.1 INTRODUCTION

In this chapter we are going to discuss about the design architecture of the secure SEPA banking system, where we are going to provide banking services to our clients. We are working on web services for the clients within the SEPA and applicable in Euro region. Clients can perform transactions by using SEPA banking system. The client will also be able perform the transactions when he is visiting a sale point by using SEPA smart cards. SEPA banking is an ongoing banking project at the SecLab (Security Lab) ICT KTH and it has three important modules. These modules are:

- SEPA Cloud and Portal module
- Web servers and services for SEPA Financial Servers Administrators
- Web Services for SEPA Web Users

In this research, our focus is on Web Services for SEPA Web and smart card users and component involved in it. We will discuss the SEPA bank web services: user registration in SEPA bank, transactions, payments, and currency conversion. In another section, we will discuss SEPA POS devices.

5.2 ARCHITECTURE AND COMPONENTS

In our research, we are going to give services to web clients/users that are going to use SEPA banking system. However, before using SEPA web services, the customer must sign into SEPA banking system. The user can be registered in the (Identity Management Server) IDMS system with the specific bank mentioned in the registration form. After the registration, users can access SEPA banking services. We will discuss SEPA banking web and smart card services in the next chapter.

5.2.1 SAFE SYSTEM

SAFE System is developed in the SecLab KTH. It is a secure banking system where the client will have access to the server and can perform financial transactions. SAFE System is accessed in two ways: one is through GPRS and the second way to connect through Internet SAFE System and its components are shown in the following Figure 6.
5.2.2 SAFE COMMUNICATION SERVER

We discussed the SAFE system and its components involved with the SEPA banking system. SAFE communication server is connected with POI/POS device either by GPRS or through wireless. User will swap their SEPA smart card, their information will be accessed. POI device is connected to SAFE Communications Server. Furthermore, it connects to the SAFE Payments Server. After overall communication the payment shall be processed [28].

5.2.3 SEPA BANK SERVER

SEPA bank server has an organized hierarchal structure. We have National servers for SEPA and individual SEPA Bank servers. Every bank server is connected to SEPA National Server when some transaction has been done. Each SEPA National server is connected and communicating to SEPA Bank main server. This step is taken when we are going to perform transactions across the border. When transactions are domestic, then only SEPA Bank servers are in communication with each other, they don’t need to update or communicate with SEPA National server. Security between different servers and messaging are deployed and come under the SEPA Financial Servers [17].

5.3.3 PORTAL SECURITY ADMINISTRATION

SEPA Portal Security Administration server is the first step to get into the SEPA banking system. To get to the services for web users, as well as for the admin who is managing the SEPA banking
system servers, all have to pass thorough Portal Security Administration. Portal Security Administration is used for multiple tasks; it is managed by the portal administrator and is also responsible for assigning the roles. Portal Security Administrator consists of web server, proxy server, PEP server, and Virtual Private Network (VPN) [19].

5.3.4 **Web Server**
Web servers are basically used to access SEPA banking web services and clients registration. Web server is providing a web interface to users and clients. User is connected to the cloud station and further it is communicating via web interface with the web server.

5.3.5 **SEPA Customers**
SEPA Customers/ Clients are users who use SEPA Bank web services. There are two ties of customers/ clients. One who is using the SEPA Banks services by connecting through web pages under the web servers. A customer can perform transaction, conversion, payment and can check balance of their accounts. The second potential customers are by using SEPA Bank smart cards in POI/ POS. POI/POS devices are connected to SAFE system developed at SecLab KTH.

5.3.6 **SEPA Web Wallet**
SEPA Web Wallet is used for mobile and web wallets. Clients who want to access the SEPA Web Wallet will communicate via SEPA banking system by using the web server. For confirmation, the client uses SEPA smart cards. SEPA smart cards are discussed earlier.

5.3.7 **SEPA Mobile Wallet**
SEPA Mobile Wallet is another banking service for mobile clients/customers. Mobile wallet clients are connected to SEPA system via smart phones and use their SEPA smart cards. All financial transactions are updated in the SEPA web wallet banking. SEPA mobile wallet is also under development of Secure SEPA Mobile Wallet Clients [18].

5.3.8 **SEPA POS/POI Device**
SEPA Point of Sale or Point of Interaction devices are the machines which are used in the SEPA banking project. When a customer/client visiting a shop or some other business place and want to do payments, he/she uses his/her SEPA smart card to do the payments.

As shown in Figure 7 customer is using his/her SEPA smart card in POI device. POI device is connected through GPRS or wireless to the SAFE System and thus he/she is able to perform payments.
Figure 7: POI in SAFE System

Figure 7 shows SEPA customers interaction with SAFE system and SAFE communication server and related functions to it. SEPA POI and smart card reader are shown in the following Figure 8.
Figure 8: SEPA POI smart card reader
CHAPTER 6: IMPLEMENTATION AND DEMO OF THE SYSTEM

In this chapter we are going to discuss implementation of the Secure SEPA Banking system services for web and smart card clients in cloud environments. We will discuss web services implementation and some services developed for POI devices. We are going to discuss the technologies used during our research.

6.1 CONTENT MANAGEMENT SYSTEM (CMS)
CMS is a tool which is used for modifying, editing and publishing the content and keeping maintenance of the main interface. It manages workflow and it helps in developing a website flexible to publish the content over website. CMS has two main elements:

- Content Management Application (CMA) is used for front end interface and allows user to make changes and addition in the interface without the web developer help.
- Content Delivery Application (CDA) is used for compilation and updating the website.

CMS only requires knowledge of HTML and CSS to work in, and it is developed itself in PHP [21].

6.2 ECLIPSE C++
Eclipse is a multi language supporting software a workspace and extensive plug-in system. Eclipse is written in Java and can be used to write and develop more applications by installing extensible plug-ins. After installation of plug-ins, a developer can develop applications using C, C++, Python, PHP, Perl and many other programming languages [22]. Eclipse C++ SDK is used here in our research for developing the POI/POS client bank services which already has been developed at SecLab KTH. After the development, we upload the SDK into POI device and by using smart card we can access SAFE System by using GPRS or Wireless.

6.3 INIT TOOLS
Init Tools is an interface developed for making the make file which is further used for POI device. It is an .exe file and works like an input source files. Developer can add libraries and files, along with the source code which are required for building a make file. After building a successful makefile.exe, we run that and compile it using init tools.exe. There are different fields and options in this application. Suppose here is some basic information of the POI device, whether it is properly connected with the system or not. We can see the POS device Type, baud rate, protocol version, language setting etc. Communication port and baud rate are the two important elements in this tool, by which we can see the device thorough which it is physically connected with the system and doing communication on which baud rate. In the second part of this tool we upload different libraries and files and after that we can build a make file [23].
Init tools are shown in Figure 9.

Figure 9: InitTools.exe

6.4 Apache, MySQL
Apache Tomcat is open source web server which facilitates Java server pages to run. It provides a HTTP web server platform to run Java servelets and Java server pages. In our research, we have used Apache Tomcat to run our web pages. Besides that, we have used MySql to create our Data Base, as we are using Data Base tables for SEPA banking web services.

6.5 Web Pages and Templates developed in JSP, HTML
We have used JSP and HTML for creating SEPA web portal. The main cloud portal is developed in HTML, PHP, and HTML. We can deploy a product in a project, because of support of JSP, servelet container, efficient and compatible web server. We have used here Apache Tomcat for that purpose. JSP can deliver HTMLX and XML content by mean of OutputStream. Besides that, it is also user for data types as well. In Figure 10, we show the main page of our Cloud Secure Administration [20].
6.6 Demo of the System

In this section, we will describe and through some figures show how our system works. In this research we have developed services web clients and users. Therefore, we will show to our audiences and users how they will use the services. As stated earlier, there is main SEPA web portal. After login in the main portal user will find tab button under “Secure Cloud Banking” as shown in the following Figure 11.

After clicking the button, it will take user to main menu. This menu consists of Registration, Accounts, and Services. We will go in more details one by one of these services.
After registration, user will be able to open account. User will have to access Accounts tab. Accounts page is shown in Figure 13.

As shown in Figure 13, user can register account, log into an account and also list of accounts should be shown. Inside the list of accounts, user can delete his/her account. After this function, the user can add an account by giving the Account No and PIN. It is shown in Figure 14:
Figure 14: Account Page

By entering Account No and PIN user can see details of his/her account.

In another figure, we have shown bank services to the user. In these services, there is transaction, payment, and services.

Figure 15: Bank Services

After checking the account details user can do transactions with another accounts. It is shown in Figure 16.
6.7 CONVERSION

Figure 17 shows currency conversion. User can convert Euro into Danish Kroner (DEK), Norwegian Kroner (NOK), or Swedish Kroner (SEK) currencies.

6.8 MAKE FILE FOR PROJECT

Along with the web services, some work has been done for POS/POI device for the smart cards. The tool which is developed at SecLab ICT KTH, called Project Configure Tool, which is used to create C project makefile. This tool is very easy to use and developer can input their files and
libraries, after successful compilation makefile is created which is further used for the next step. Init tools and its related process for further POI device are shown in the following figure.

As shown in Figure 18, there are different fields for input fields. Developer will provide the correct files and libraries paths in the respective field. After giving the input files, makefile is created and then loaded to the POS/POI device.

![Figure 18: Init Tools for POI Devices](image)

After successful compilation and creating makefile, the next step is to feed information in the POI device. This information is shown in Figure 19.
In the above Figure 19, there is information about Merchant who is using the system, SAFE Account; option is available for SAFE Mobile, the port number by which the SAFE System and POI device are communicating with each other. As discussed earlier, there are two ways of communication between the SAFE System and POI device.

- GPRS
- Wireless

It is shown above that system is communicating through wireless protocol, an uploading SDK and connecting to the SAFE System. Here in our research project we have worked as shown in Figure 20.
Figure 20: POI Device in Communication with the SAFE System
CHAPTER 7: FUTURE WORK

In this research under the supervision of Professor Sead Muftic the whole team have started project from scratch. There are many components in this project: SEPA portal, SEPA Server, Mobile Wallet and SEPA web clients.

In this research we have developed web services for the web clients in SEPA using Secure Cloud environment. Client enters in the SEPA web portal and, after registration and opening bank account, he/she can use banking services e.g (payment, transaction, conversion). These services are developed at the basic level. Some security aspects should be provided in the future work. The currency conversion should be converted to online exchange, where the client can get the updated rates from the currency exchange rates. Currently we have connected the rates with the databases.

The second most important future work is for smart cards where they will be used with POI devices. The POI device is connected with the SAFE system, when a user swaps a card. The POI device will communicate with the SAFE System and card information shall be accessed. User will be able to check and see his account, credit/debit card information, issuer, amount in the bank account, 16 digit card number, user name, date of issue and expiry etc on the device screen.

Future work in this project is all about components SEPA parts (SEPA Portal, SEPA Banking Web servers, Web clients and POI Application for smart cards should be integrated in one SEPA banking application and shall be implemented in the cloud environment.
References


[9] Jan Van Den Akker Chapter “Principles and Methods of Development Research”, University of Twente, Netherlands


[23] InitTools.exe, developed at Security Lab (SecLab), ICT KTH, Sweden


[27] Project Configure Tool for makefile.exe, Developed at SecLab, ICT, KTH

[28] SAFE Server, “SAFE Banking system” Developed at SecLab, ICT, KTH Sweden
APPENDIX A: ABBREVIATIONS AND ACRONYMS

ACC.No  Account Number
ATM     Automated Teller Machine
B2B     Business to Business
BIC     Business Identifier Code
CAS     Common Approval Scheme
CDA     Content Delivery Application
CMA     Content Management Application
CSG     Cards Stakeholders Group
DECS    Data Exchange for Cash Services
DSS     Data Security Standards
ECB     European Central Bank
EEP     European Economic Policy
EMV     Europay, Master card, Visa
EPC     European Payment Council
ESTA    Security Transport Association
EU      European Union
IaaS    Infrastructure as a Service
IBAN    International Bank Account Number
IDMS    Identity Management System
MiFID   Markets in Financial Instruments Directive
NIST    National Institute of Standards & Technology
PaaS    Provider as a Service
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI</td>
<td>Payment Card Industry</td>
</tr>
<tr>
<td>PCI DSS</td>
<td>Payment Card Industry, Data Security Standard</td>
</tr>
<tr>
<td>PDP</td>
<td>Policy Decision Point</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identifier Number</td>
</tr>
<tr>
<td>POI</td>
<td>Point of Interaction</td>
</tr>
<tr>
<td>POS</td>
<td>Point of Sale</td>
</tr>
<tr>
<td>PSE</td>
<td>Payment Selection Environment</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SCF</td>
<td>SEPA Cards Framework</td>
</tr>
<tr>
<td>SCT</td>
<td>SEPA Credit Transfer</td>
</tr>
<tr>
<td>SDD</td>
<td>SEPA Direct Debt</td>
</tr>
<tr>
<td>SECA</td>
<td>Single Euro Cash Area</td>
</tr>
<tr>
<td>SEPA</td>
<td>Single Euro Payment Area</td>
</tr>
<tr>
<td>VVM</td>
<td>Virtual Machine Manager</td>
</tr>
</tbody>
</table>