Secure Over the Air (OTA) Management Of Mobile Applications

Dinakaran Rajaram

KTH-Royal Institute of Technology
School Of Information and Communication Technology
Communication Systems

Master of Science Thesis

Stockholm Sweden 2012

Acknowledgement

I am very sincere and really thankful to my supervisor Mr.Sead Muftic to give me this wonderful opportunity to do Master thesis research under his supervision. He shared his experience and his valuable knowledge. Because of his proper guides, I could able to finish my mater thesis in six months of time period.

My hearty thanks to Mr. Hao Zhao, Ms.Chenchen Yuan, and Dr. Feng Zhang . They dedicated their valuable times to guide me. A special thanks to Mr. Hao Zhao for providing the technical guidance and sharing his ideas to handles the SecLab equipments. I would like to thank all my colleagues in SecLab especially Mr. Majid mumtaz for sharing his valuable ideas.

I am really thankful to Mrs. Alphonsa Lourdudass for her guidance throughout my life span in Stockholm. I would like thank my parents for their kind support throughout my life.

Dedication

To My Parents
Mr.K.Rajaram
&
Mrs.R.Selvarani

Abstract

The Thesis report analyzes the possibility to store the application inside a secure environment in over the air Environment. The report clearly explains the details about the attributes which are placed in the over the air application management. Different forms of secure elements and how it can be placed inside the secure micro SD card have been discussed. The report gives the clear idea about secure micro SD card architecture. The report describes the OTA (Over the Air) components, Roles and also the process to manage the applications in OTA environment. The report also gives the clear about the protocols ISO 7816-4 which is used to communicate the handset with secure micro SD card. The communication concepts like establishing secure channel between the handset and secure micro SD card also has been discussed. Moreover, secure channel attributes are also discussed. They are Creation session key, MAC Operation and generation of derivation data. Secure micro SD card API‘s are also discussed which is used to communicate with the secure micro SD card .Some of the implementation work has been done by this research. They are

- Constructed the Design of Trusted Service Manager (TSM) and Service provider.
- Implemented the Functionality of TSM Server (Download Function) and tested the Functionality whether the end terminal (Android Phone) has been able to use the function properly.
- Established the secure channel between the Android phone and secure micro SD card.
- Loaded the sample application inside the secure micro SD card.

Table of Contents

List Of Figures

List Of Tables

Symbols and Abbreviations

OTA - Over the air
TSM - Trusted Service Manager
SP - Service Provider
PIN - Personal Identification Number
UICC –Universal Integrated Circuit Chips
SIM - Subscriber Identity Module
MAC – Message Authentication Code
APDU- Application Protocol Data Unit
API - Application programming Interface
SMS - Short message service
DES – Data Encryption Standard
RSA – Ron Rivest, Adi Shamir and Leonard Adleman
CBC – Cipher Block Chain
ECB – Electronic Code Block
ETSI – European Telecommunications Standard Institute
ISO - International Organization for Standard
HTTP – Hypertext Transfer Protocol
SAFE –Secure Application for Financial environment
EMV – Euro pay, Master card, Visa
NFC - Near Field Communication
RAM – Random Access Memory
ROM – Read Only Memory
EEROM – Electrically Erasable Programmable Read Only Memory
CPU – Central Processing Unit
JSP – Java Server Pages

1.Introduction

The Introduction part describes about the background research analysis which gives the background knowledge about the research. Then problem statement, motivation and Methodology also are described in this part. Over The Air (OTA) is a technology that has gained wide acceptance and development in recent times. This thesis de-scribes the Over the Air Communication among the TSM (Trusted Service Manager) and secure micro SD card. The main Challenges are to establish the secure way communication between the android Phone and Secure micro SD card .Here the Android phone act as a mediator between TSM and Secure micro SD card. The introduction part gives the design and structure of the TSM and also describes the various components in Over the Air provisioning. Then it describes all the security breaches which has been highly possible to occur among the components of over the air provisioning and possible security measures also be discussed in this part.

1.1 Background

Nowadays, the growth of mobile technology is tremendous. Human cannot able to live a single day without a mobile. So Mobile devices are having close attachment with human. All off the mobile phones are used for communication. (i.e.) calls, Sending Messages. But Considering the Smart Phones, They are also been used to do some computing operations which can be done by computers. Moreover, Smart Phone has large numbers of applications inside it. Some of them are banking application which has been used for financial transactions which is used to transfer sensitive and confidential data. But if a security features of data which has been stored inside the smart phone is questionable. If consider the case like if the smart phone has stolen. But the Phone owner hasn't log out of his bank transaction application. In that case, there is a strong possibility to steal the Credential information from the Phone. Even though, the smart phone user uninstalls the banking application, there is a possibility to get back the phone information by using the data recovery method.

1.2 Overview of OTA (Over the Air) Management

The OTA management means that the communication bodies like server, client should communicate each other by using wireless medium. Some of the components of OTA Management.

Service Provider (SP); The Applications which loaded inside the mobile phone are provided by the service Provider. (Example) bank application, restaurant application, etc…As for now the Mobile applications are stored inside the phone itself. But it can be leads to misuse the data. Banking applications have some credential data which should be forbidden to others like password, PIN. Moreover, service provider stores their applications inside the Trusted Service Manager. Mobile device downloads the application from Trusted Service Manager. Here the Service Provider should check the authenticity of the Trusted Service Manager.
Because someone can be pretend as Trusted Service Manager to collect information from the Service Provider which leads to Identity theft.

Trusted Service Manager (TSM): TSM administrates all the applications which are coming from all kinds of service providers. TSM should verify the authenticity of Service provider and also their applications. Because the application may contain some malicious logic .This can be done by TSM administrator which is a part of TSM. The other part of TSM called TSM server from where the service provider's applications are stored. Mobile device can download the Application from TSM server. (Example) Play store for Android, apple store for Apple.TSM administrator should also verifies the authenticity of TSM server and also it should be performed vice versa.

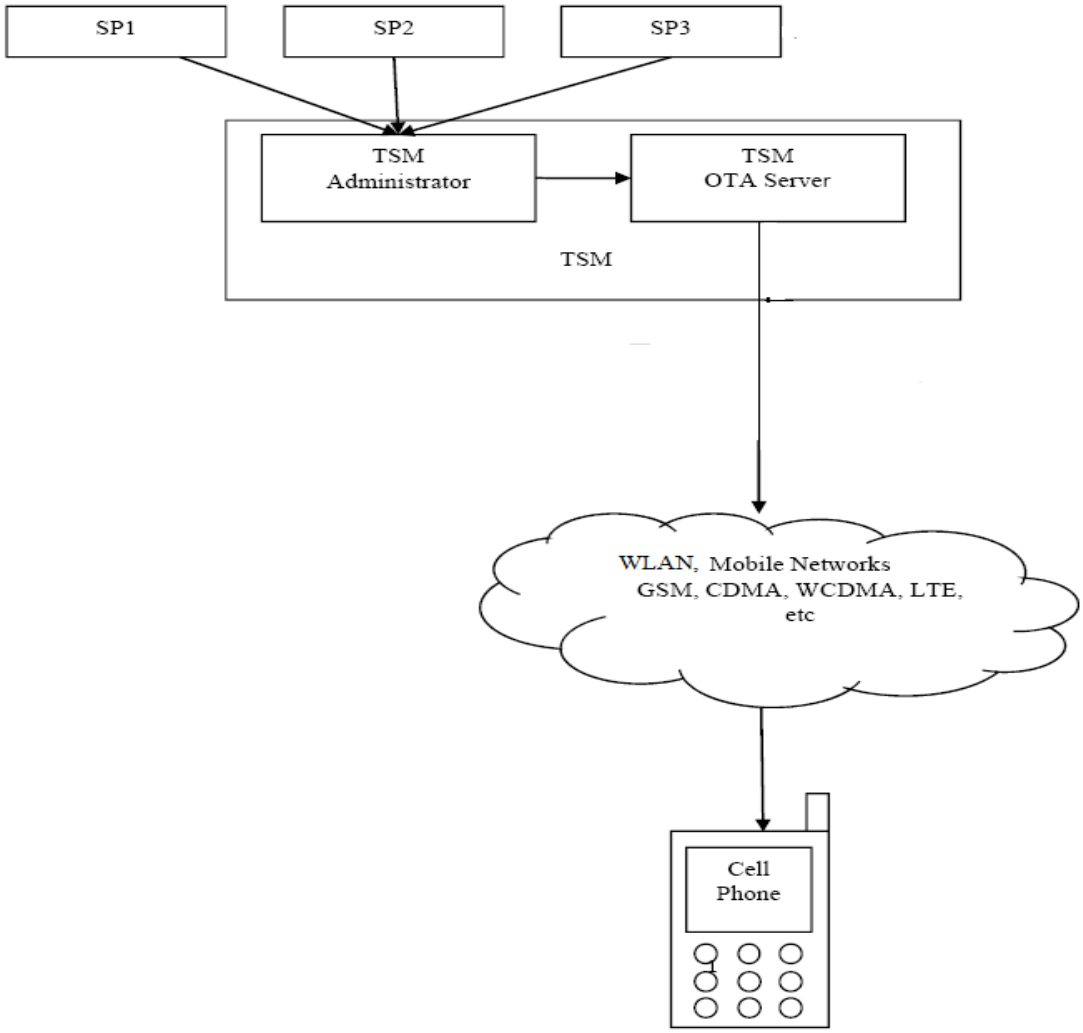

Figure 1 1Overview of OTA Management [4]

Cell Phone: Mobile phone is the final terminal which has been used to store the application inside the phone memory (or) external memory disk. But it would be insecure. Consider the sensitive data credentials like password, PIN which can easily steal from mobile phone.

1.3 Problem Statement

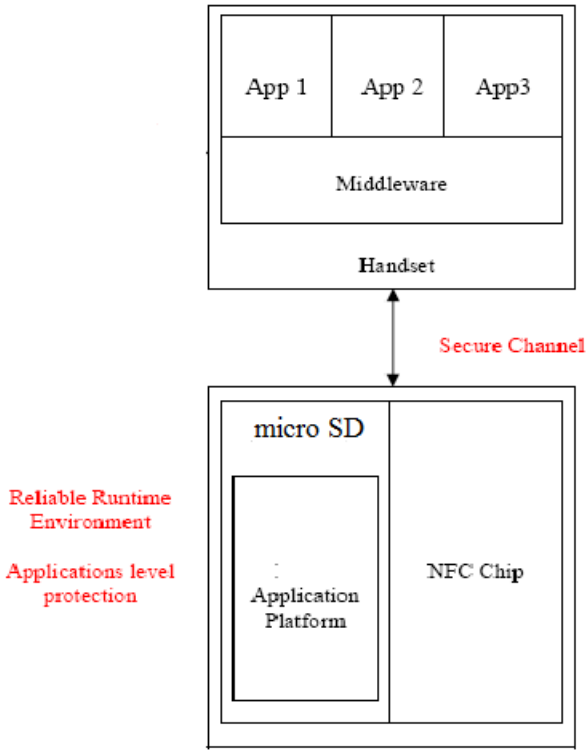

Figure 1 2 Establishment of Secure Channel between Handset and Secure Micro SD card [4]

Consider the application is transferred from TSM server to smart phone and the applications are stored inside the smart phone. Even though, The TSM server verifies the authenticity of smart phone user and transfer to smart phone. But still it has the possibility to steal the information from the smart phone. By installing some spy software inside the Phone, one can track the smart phone activities and also collect the credential information like password, PIN etc. Moreover, if the application data are removed from smart phone, even there is a possibility to track the information by using the Recovery software. This is highly challenging thing for financial transaction kinds of applications. In order to avoid those problems, this research can be done. One of the final products of this research is Establishment of secure channel which provide a secure connection between the smart phone and secure micro SD card. By using the secure channel the application is stored inside the secure micro SD card. First Step Before sending the application is establishing the mutual authentication between the smart phone and secure micro SD card. That can be done by shared symmetric key between the smart phone and secure micro SD card. The operation of secure micro SD card is performed in closed environment. So no one can be able to monitor the operations of secure micro SD card. This is the good method to avoid the stealing of information from smart phone. Because the credential things (data, key, etc.) are stored inside secure micro SD card.

1.4 Motivations

It is very harmful if the applications are stored inside the phone. Suppose if anybody steals the phone they can steal the valuable information of the application. Consider the banking application, there are several credential information are involved like password, PIN etc. But Storing the Application inside the secure micro SD card is safe. Even though, android phone which is communicated with the secure micro SD card cannot be able to monitor the process of secure micro SD card. It avoids some problems,

- **Security Problems:** Data stored in secure micro SD card is safer. If an attacker cannot able to get back the information even he used the reverse engineering technique. Moreover, the secure micro SD card is tamper proof, so it is very hard to the attacker to destroy the card.

- **Time Problem:** Consider the secure application which stored inside the mobile phone. In order to provide the secure features of each application, it's very time consuming process and also the security feature of each application defers. But establish secure channel with secure micro SD card provides more security. So the developer can spend less time on application's security features.

- **Space problem:** If consider the case, without implementation of secure channel with secure micro SD card. Then developer should concentrate more on application security. Then each application will occupy more space for security code and libraries.

This research will be more concentrate on establishing secure channel with secure micro SD card which eliminates all the issues mentioned above. Even though, security features for each application is mandatory. This will be reduced the burden of it.

1.5 Limitations

Intial analysis of this research focused on doing the research with UICC based SIM cards. The UICC chip environment suppots multiple applictions can reside inside the SIM card. It provides the run time environment for multiple applications. But the network operator have the control over the SIM card . They have secret for the SIM card. without having the key The normal user cannot be able to enter their application inside the SIM card. So that is the reason to do the research by using secure micro SD card . But secure micro SD card provides the same Security which the smart card provides. But secure micro SD card will not support the mutiple applications inside it. So it is called mono band.As for intial study shows to do the research in SIM need to have more resources.

Moreover, The network operator should also have an agreement with each and every service provider to use their services. This is really a large scope project which should not be possible to do within the research peroid. But these are things which will be the continuation of this reasearch. This research will be thestep stone to do these kinds of research in larger scales.

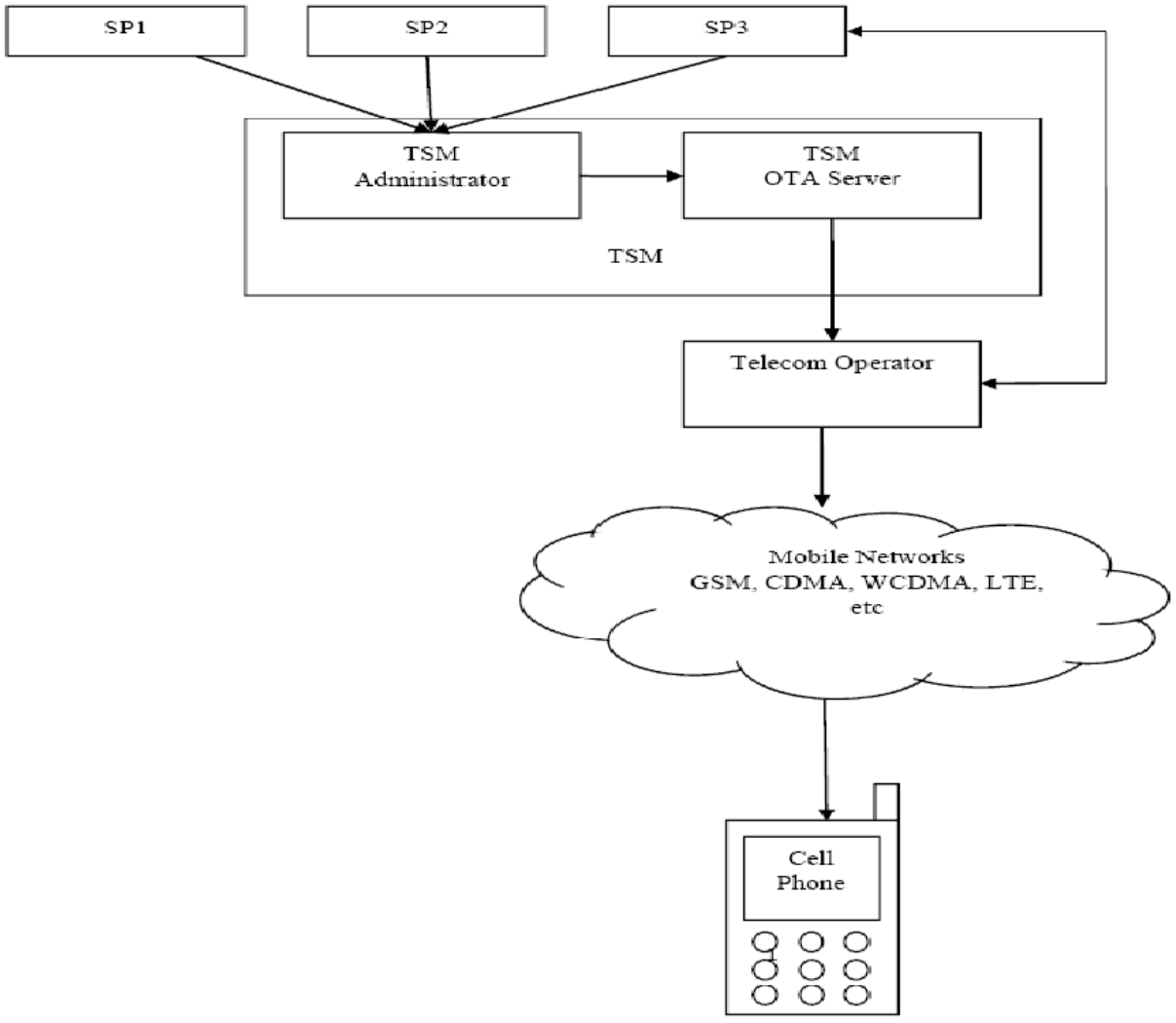

Figure 1 3 Network operator control over the OTA environment [4]

1.6 Scope

The Scope of this research is only focus on Establish the secure over the air (OTA) Communication between Trusted Service Manager (TSM) and Secure Micro SD card. For that, first The OTA channel established between the TSM server and The Android Phone which holds the Secure Micro SD card. Finally establish the secure channel between the android phone and the secure micro SD card.

1.7 Methodology

In this research, some modules have been designed, implemented, and tested. So methodology of this research belongs to creation of an artifact. The methodology has been described by below steps

- Construct the Design principles of Trusted Service Manager (TSM) and Service provider.

- Implement the Functionality of TSM Server (Download Function) and testing the Functionality whether the end terminal (Android Phone) has been able to use the function properly. Then checks Function has been executed successfully.
- Establishing the secure channel between the Android phone and secure micro SD card. It contains below steps.
  - Generation of Host and Card challenges.
  - Creation of session Keys.
  - Calculation of Card and Host cryptograms.
  - Secure channel establishment by using MAC operation.
- Testing the secure channel establishment by verifying APDU commands. (Example) If the card returns APDU response 9000, the Command which has been send by Android has been successfully accessed by the card.
- Loading the sample application inside the secure micro SD card and test the presence of the application inside the card.

The major goal of this research is to provide secure Over the Air (OTA) provisioning between the TSM server and Secure Micro SD card. But the Goal can been divided into two sub goals

- Provide Secure OTA provisioning between the TSM and Android (Communicator with Secure micro SD card).
- Provide the Secure OTA provisioning between Android and Secure micro SD card.

The reason for the division is the Secure Micro SD card has tiny processor. So it is very difficult to perform all the operations which need to establish the secure channel. So to reduce the work load of the secure micro SD card processor, the heavy functional operations are performed inside the Android phone. But the credential information (key, generating cryptogram) are performed by the secure micro SD card which consider as more secure. It is impossible to get back the data from secure micro SD card. The operations inside the secure micro SD card are invisible. Android phone access the secure micro SD card by using APDU commands. The Android phone cannot be able to view the operations inside the secure micro SD card. Android just send the instruction to secure micro SD card. The instructions are known by secure micro SD card which is called Micro card API [5]. The secure micro SD card processes the instruction and return 9000 if the instructions are successfully accessed. So the external word cannot be intrude the secure Micro SD card operations and also impossible to steal the information.

1.8 Objectives of This Research

This research focuses on the secure way of transferring application and stores the application in secure environment. During this research, secure way of storing an application is achieved. The structure of this report contains 6 chapters. The 2nd chapter discuses about the mobile applets, secure element, management of mobile applications, Overview of OTA architecture and existing solutions. Roles of components placed in OTA architecture and protocol procedure used in this research have been discussed in 3rd chapter. The 4th chapter explains the design, concepts and implementation of the prototype which has been developed. Conclusion and Future work has

been discussed in 5th chapter. The 6th chapter contains all the references which are used in the whole research.

1.8.1 Relevant Standards and some important Background Materials

The initial study is based on the USIM cards. The functionality of the USIM cards and how the OTA communication has been implemented in USIM cards .For example, to analyze the SMS APDU commands which give some knowledge about the SMS communication by using the network operator services and also give some basic knowledge about the SIM toolkit. Though the scope of the thesis contains manipulation of application, the SMS APDU commands give the initial way of communication among the entities [5].

Then it is very important to know about the OTA management to implement the Over the air (OTA) communication. If suppose a new application has been launched on USIM, it is important that USIM should also be reacted based on the new application .This article produces some kinds of USIM management [6].

This material is used to know about the basic structure of the OTA management component like TSM administrator, TSM OTA server, Service provider and how they interconnect with each other entities and also it provides the knowledge about a secure wallet application which is not in the scope of this thesis[4].

For the development of the secure channel, this material is useful. This material gives the overall structure about the secure channel mechanism, cryptography technologies (For Example 3DES-CBC, 3DES- ECB)which have been used for this development, MAC algorithm which are used to construct cryptograms and gives the Knowledge about the encryption key and Mac Key[8] .

This material gives Holistic view about the Micro card API which is very useful to communicate the Secure Micro SD card from android mobile. This material is very useful in the implementation phase [1].

2. Overview of OTA management of Mobile Applications

2.1 Mobile Applets

The over the air communication, the mobile applications are transferred from Trusted service manager to the client device. Storing the applications in client device contains two kinds of approach. First approach is storing applications inside the mobile phone. All the mobile phone has been designed to support java technology. It supports the J2ME standard. The application can been stored inside the mobile phone's memory (or) external memory stick. Though the mobile phone provides all kinds of security services, the mobile phone applications will be affected if some malicious functions are already stored inside the phone. The second approach is storing the application inside the SIM card chip (or) UICC chip (or) secure micro SD card chip memory. SUN provides micro device java environment for SIM chips. The internal executions can be done by this java technology. By using this java technology, the developers can develop application to store inside these smart card chips. So these applications are normally called java card applets. The developers no need to worry about the hard ware technology and also the hardware configurations to communicate with the smart card chips. For that the java technology defines some API's which are used to communicate with these smart card chips. These API's are converted as some instructions which have been understand by the smart card chips. The conversion from API's to command instructions are defined by some standards like Global platform, ETSI and ISO .Consider to store the applications inside the SIM chips, user needs to get permission from network operators. Because the network operators have the whole control over the SIM card. That is the reason of chosen secure micro SD card to do this research.

2.2 Secure Element

The Secure Element accommodate inside the chip which provides high level of crypto environment. The chip has its own RAM, CPU, EEPROM and ROM. The operating system of secure element is stored by using ROM. The data and Mobile applications are stored in EEPROM. The secure element's applications have mentioned by some program code.

If consider the java supports secure element, then the secure element includes all important java toolkits. In this case, the secure element applications are compiled as java byte code and stored inside the EEPROM. It is impossible to get back the data which are stored inside the secure element by using secure element. Moreover, the operations which are performed inside the secure element are invisible to the outside world. So it is difficult to track the operations of secure element and also the hardware of secure element is very strong which cannot be spoiled by any kinds of physical attacks. Secure element also designed to support all kinds of secure protocols like DES, Triple-DES, and RSA etc.

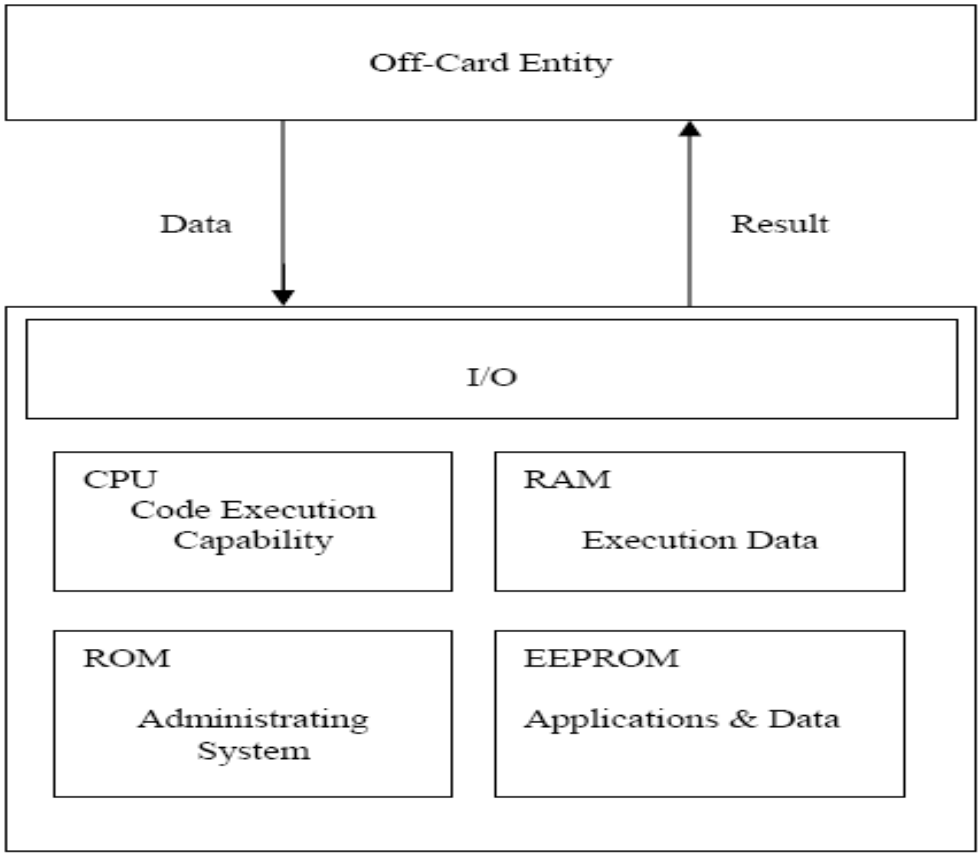

Figure 2 1 Smart Chip Internal Structure [4]

2.2.1 Different Forms of Security Domain:

According to the new technologies, the Secure Element is in three different forms.

Inside the handset: The Secure element can be mounted inside the motherboard of a handset or else it has a connection with the motherboard.
Inside Secure Micro SD card: Micro SD card chip has the Secure Element inside it.
Inside a SIM: Secure element is the most important part of the SIM card.

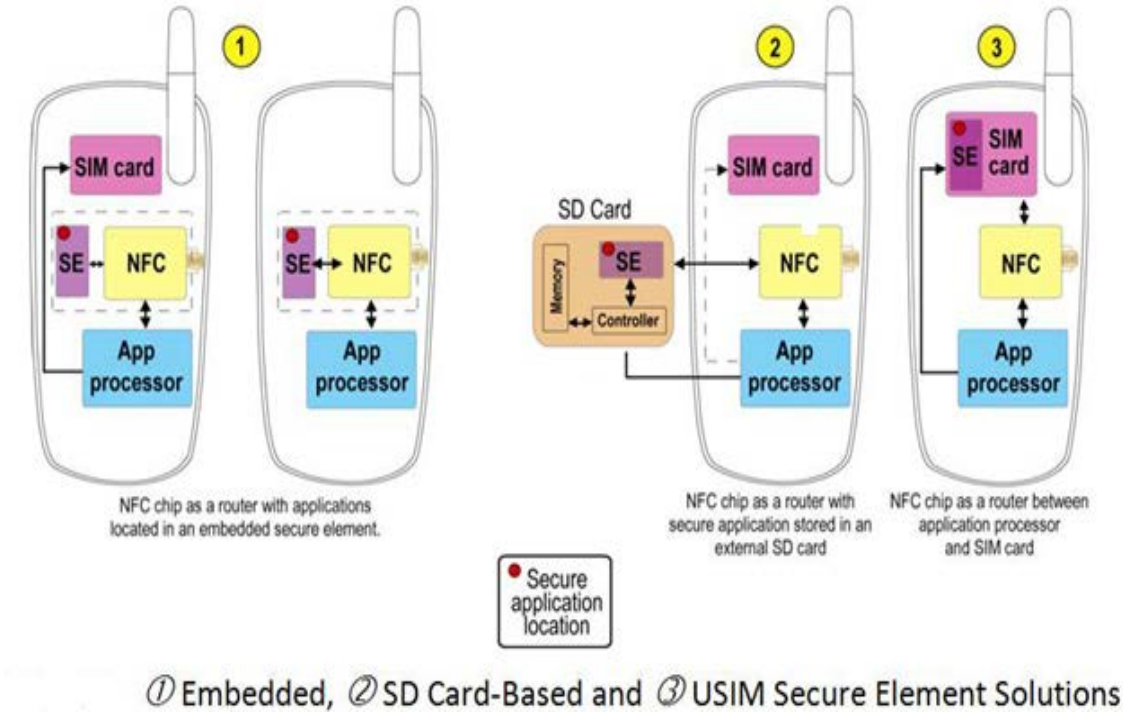

Figure 2 2 Different forms of secure domain [9]

2.2.2 Secure Micro SD card:

Secure Micro SD card has a massive storage capacity with the secure element as set (chip and the card reader) .it typically act as a smart card. But in smart card we can store different kinds of applications and the applications are separated by different kinds of firewalls which is normally called as security domain [2]. But secure micro SD card cannot able to store multiple applications. So it is called mono-band [11].

Here is the reason for chosen secure micro SD card to do the experiment. In order to do the experiment in SIM card, we need to get permission from network operators. Because they have the control over SIM to do the manipulations of data inside the card. So it is very hard to get the permission from network operators. Moreover, secure micro SD card provides the same security functionality which has been provided by the smart card and also it can be accommodated with any kinds of smart phone devices slots [11].

The Characteristics of Secure Micro SD card [11]:

1. Flash memory Space: 1GB/2 GB.
2. Functionality of Smartcard depends on:
    a. EEPROM with 36KB free space
    b. Global card platform 2.1.1 and java card 2.2 which contain Operating System with Security Features.
3. The interfaces for the platforms of hosts are based on ISO standard 7816 have been implemented by using similar drivers.
    a. Windows and windows mobile.

b. Linux.
c. Blackberry.
d. Android versions.

4. Other security features:
    a. 2048bits/1024bits/512 bits RSA algorithms.
    b. DES standard and Triple-DES algorithm.
    c. SHA1 hash functional algorithm.

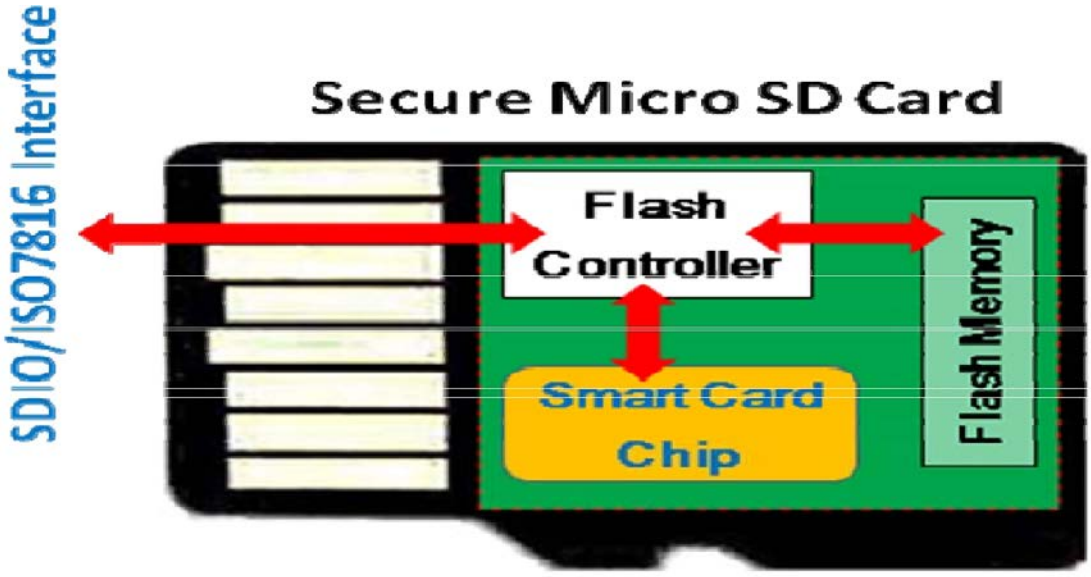

Figure 2 3 Secure Micro SD card Internal structure [11]

Major Security Functionality of Smart Chip:

1. Mobile Single Sign-on.
2. Signature for E-mail/ Encryption Functionality.
3. Possibility of authentication with two factors (Card and PIN).
4. Provide Strong authentication and also access control.
5. Provide Key for Mobile Payment (lottery for mobile payment) [11].

2.3 Management of Applications

The management of an application contains several kinds of Steps in the client end. They are

2.3.1 Selection

In this OTA Architecture TSM is Server and at the beginning, android phone is considering as Client. First the Client should authenticate the Server. Then the server's applications are displayed and then the client can choose their desired application from the display list. Then application will be installed inside the android phone. The next step is to install the application inside the secure micro SD card. For that the second selection will be processed. So first the user should authenticate him with the android phone by using some PIN (or) password kind of authentication. Then the user should choose the application that which one he wants to install inside the secure micro SD card from the display list. The display list has shown the list of applications which is stored inside the android phone.

2.3.2 Installation

The second step after selecting the application is installing the application to secure micro SD card. This also can be done by two steps. First Step, The application is installed inside the android phone. The second step is to install the application from android mobile to secure micro SD card. During the first step the application data can be transferred as stream data by using socket communication. During the second step, the stream data can be transferred by using APDU (Application Protocol Data Unit) Instruction. Because the card only knows APDU instructions. The Installation process is done by a secure manner. The reason is during the First Step mobile device is authenticated TSM server to download the application inside android phone. Second user authenticates the Android phone and also secure channel has been established with the secure micro SD card. Then through secure channel the application has been transmitted inside the secure micro SD card.

2.3.3 Verification

The verification is just to check whether that the application is successfully loaded inside the secure micro SD card (or) not. Because the Communication between the Android phone and secure micro SD card is done by transferring APDU instructions. So the operations which are performed between Android phone and secure micro SD card are invisible to user. Based On response from card only we determined the result of sending command execution. To confirm loading operation, the applet ID can be send by the APDU to select the Applet. Each applet has an ID which is called applet ID. If the selection of applet is executed successfully, then the application is successfully loaded inside the secure micro SD card.

2.3.4 Deletion

This is the Final function which can do after installation of application inside the secure micro SD card. Every action should perform after establishment of secure channel. Because in that part mutual authentication between the android phone and secure micro SD card is implemented. So it will give the secure path for further transaction.

2.4 OTA Architecture

The major components of OTA management have been discussed above. But above all some other components also needed for the functions of the OTA management. The administrator has a control over these components and has the control over it.

2.4.1 Content Management Server

The content management server should maintain the applications which are stored inside the TSM server. This server should check the credibility of the applications which are resides inside the TSM server. The application should not contain any kind of malicious content which will affect the whole system. Moreover, the content management server should update the application whenever the new updates are provided by the service provider [7].

2.4.2 Database Management Server

The database server maintains the data of the user, applications which are the data are available inside the TSM server [7].

2.4.3 Authentication Server

The Authentication server determines the authentication functions and also maintains the authentication functions. For Example, consider the authentication functions as user name and password. Moreover, the server needs to store each and every user authentication credentials and maintain those credentials. The authentication server should also have expandability. For example, if a new user wants t access the TSM server, the Authentication server should also allow the new user to enroll their credentials inside the server and also allow the user to change their credentials [7].

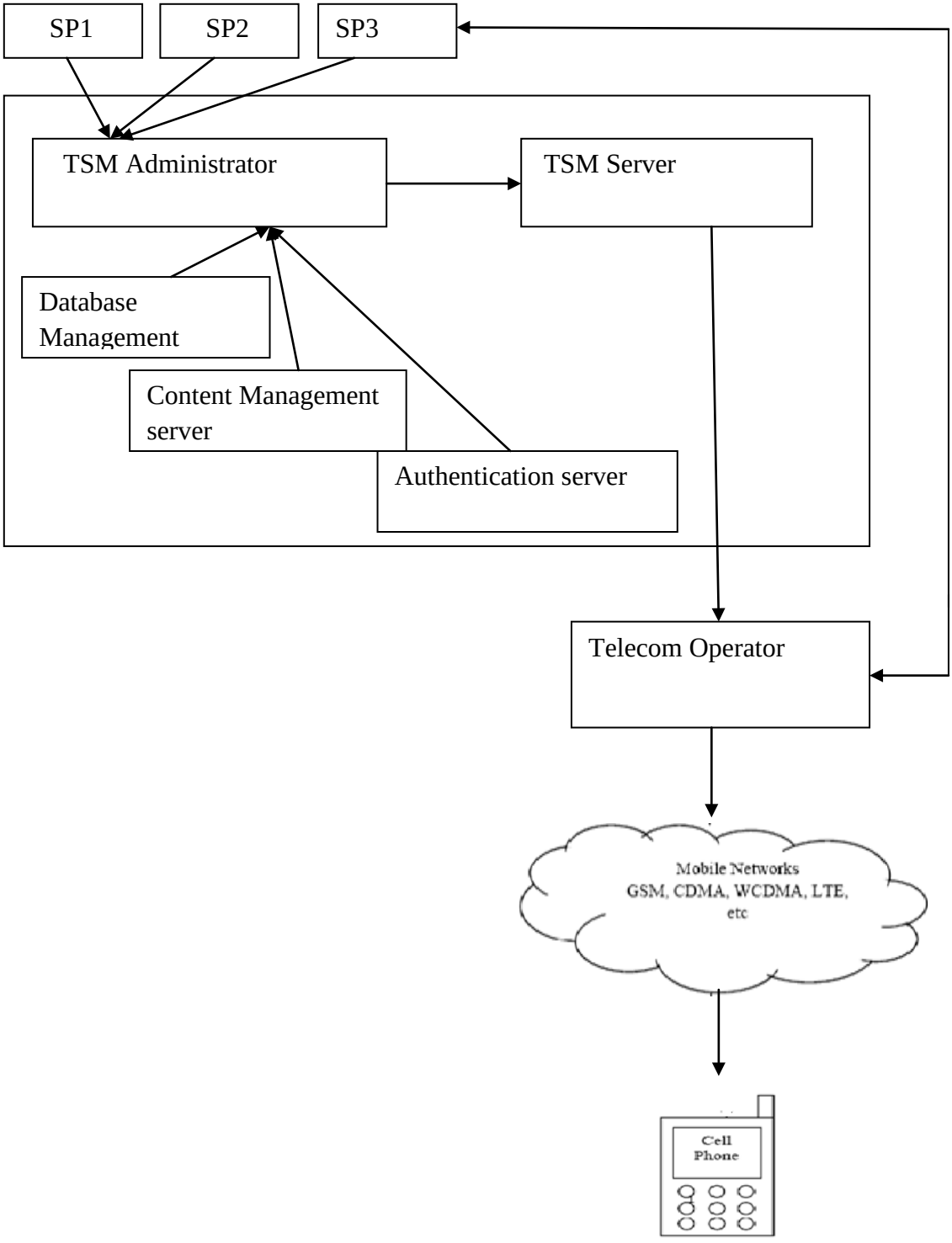

Figure 2 4 Overview of OTA architecture

2.5 Overview of existing solutions

The existing solution is storing the application inside the mobile phones by using some security mechanisms like setting password, PIN. By Using this methods, the user can provide the PIN for their mobile to protect their applications which are stored inside the mobile phone and also user can set the password (or) PIN for each and every applications .This is also possible for attackers to recovery the password by using some password recovery software. Nowadays, The TSM server does not ask any user credentials to download the applications. So anyone can pretend as TSM server to provide some malicious code to the user and also retrieve some user's credentials. But this research provides some solution like store the applications inside the micro SD card will reduce these kinds of issues.

3. Architecture for OTA management

3.1 Roles

The Roles distribution among the OTA components plays a major role. If not, it will leads to a big problem. The Roles should consider the security loop holes which should affect the whole system.

3.1.1 Roles of TSM

The TSM is the highest power authority which should have a high responsibility and high security. The TSM should authenticate the authorized user to access the TSM server. Otherwise, an attacker can easily access the TSM server and he can do some beneficiary operation which could affect the whole system. Moreover, TSM should have an interconnection with the service providers and Multinational organizations (MNOs). The TSM should verify the service provider's application whether the applications are coming from authorized party (or) not. Then TSM also should check the application of the service provider whether the applications are verified by a certificate authority.TSM should also provide end-to-end security. This is the major Purpose of the TSM administrator. TSM should also maintain the life cycle of an application. If a service provider updates their services, then the TSM should have the updated version of those services in their server. Otherwise the service provider may lose the hope on TSM. Moreover, TSM should provide 24*7 services. TSM should allow the new user to enroll inside the TSM server and define the access control for the specified user. Moreover, TSM should allocate the strong security credentials for an each individual user. It leads the authenticate user to access the TSM server. TSM should also do the deactivate services. If someone wants to deactivate the services, then the TSM should also deactivate the request user services [3].

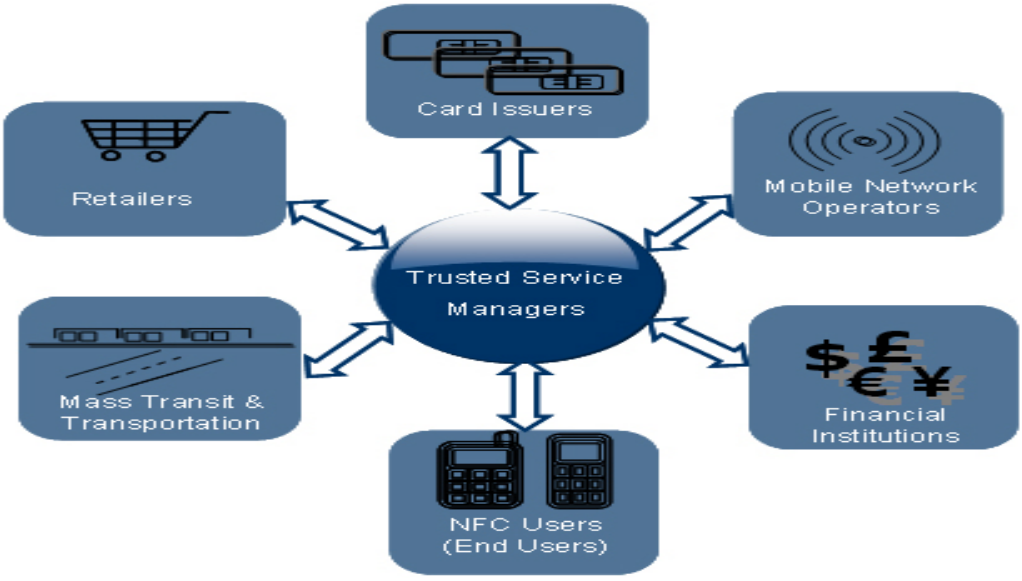

Figure 3 1 Roles of TSM server [10]

TSM should also have a connection with Card Issuers and also the network operators. Card Issuer should issue the UICC (Universal Integrated Circuit card) card which is capable to store multiple applications and also each application should be separated by security domain. TSM application should be installed inside the UICC. So card issuer should build the card based on the application supported platform. Network operators have the control over the UICC module. If the application should stored inside the card it should be permitted by network operators.

3.1.2 Roles of Service Providers

The service provider should develop their application without any security. Because it will lead to a greater disaster. The applications which are developed by the service provider should support the multiple-application platform services. For Example the services like EMV, Electronic purse, Ticketing. Those services are very useful in a business environment. Moreover, the applications should be developed by the service provider (or) by the trusted third party.

Then also get a certificate from the certificate authority. It proofs the authenticity of the application. Not only should the development of the application but also the service providers provide the regular services once the application install inside the UICC module. The service provider should also check the authenticity of the TSM server. Otherwise someone has pretended as a TSM server and get some credential from the service provider's application.

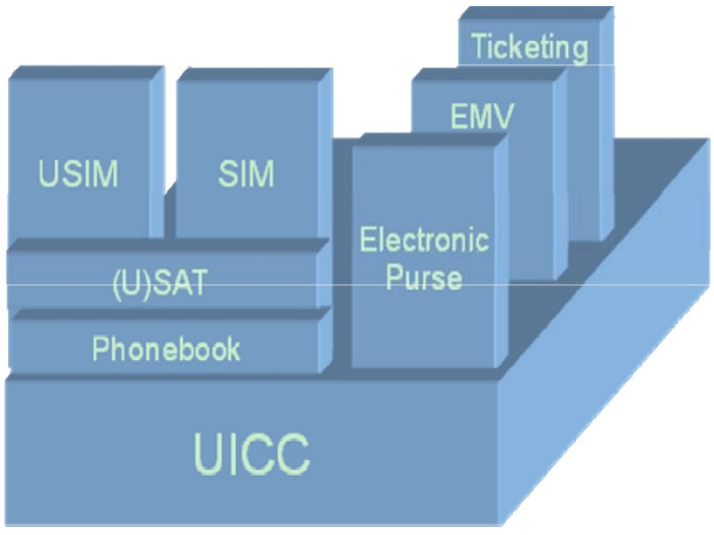

Figure 3 2 Multi application platform of UICC chip [4]

3.1.3 Roles of Client Terminal

The client should also check the authenticity of the TSM server. Otherwise someone grabs the user's information and he can pretended s the user and download the application from the TSM server. The user can download the Service provider's application from TSM by proving their authenticity and also user can change their user credentials once he/she enrolled inside the TSM server. Moreover, the user can personalize the application according to the individual user information.

3.2 Protocols of Procedure

3.2.1 ISO 7816 standard

The ISO 7816 standard commands translates the application level API's to some code which gives some meaning for each and every command. By using the meaning of these codes, the user can understand the code. This ISO standard command also called as Card Command Interface (CCI). Here the CCI commands and Application level API's are connected by using the Security application middleware. The middle ware has been implemented in java and it has been used in android environment [4].

In this research, APDU (Application Protocol Data Unit) protocols are used to translate the secure micro SD card API's. Every APDU protocol instruction gives some meaningful message which can understand by the user. The APDU protocol belongs to ISO 7816-4 standard.
The APDU protocol has the header and the body of the message. The header part indicates the category of the function to be performed and also mentioned the parameters which are needed.
The APDU is defined by hex bytes. The structure of APDU is shown below [4].

CLA	INS	P1	P2	Lc	Data	Le

Table 3 1 Structure of APDU

Representation of each attributes of the APDU [4]

Field	Length (byte)	Description
CLA	1	Class of instruction
INS	1	Instruction code
P1	1	Instruction parameter 1
P2	1	Instruction Parameter 2
Data	Shown by Lc	The information the command carries
Lc	0, 1 or 3	The length of the data body in bytes
Le	0, 1 or 3	The expected length of return data in bytes

Table 3 2 Attribute Representation of APDU

CLA: This field represents the command types which belong to ISO 7816-4 standard. The details descriptions are shown below [4].

Value	Meaning
'0X'	Structure and coding of command and response according to this part of ISO/IEC 7816 (for coding of 'X' see Table 6.5)
10 to 7F	RFU
8X, 9X	Structure of command and response according to this part of ISO/IEC 7816. Except for 'X' (for coding, see Table 6.5), the coding and meaning of command and response are proprietary
AX	Unless otherwise specified by the application context, structure and coding of command and response according to this part of ISO/IEC 7816 (for coding of 'X', see Table 6.5)
B0 to CF	Structure of command and response according to this part of ISO/IEC 7816
D0 to FE	Proprietary structure and coding of command and response
FF	Reserved for PTS

Table 3 3 Detail description of CLA [4]

b4 b3 b2 b1	Meaning
x x -- --	Secure messaging (SM) format No
0 x -- --	SM or SM not according to 1.6 No
0 0 -- --	SM or no SM indication
0 1 -- --	Proprietary SM format
1 x -- --	Secure messaging according to 1.6
1 0 -- --	Command header not authenticated
1 1 -- --	Command header authenticated (see 1.6.3.1 for command header usage
-- -- x x	Logical channel number (according to 1.5) (b2 b1 = 00 when logical channels are not used or when logical channel #0 is selected

Table 3 4Detail description of CLA [4]

INS: This field represents the functions which are used in the APDU command. The detail descriptions are shown below.

Value	Command Name
'0E'	ERASE BINARY
'20'	VERIFY
'70'	MANAGE CHANNEL
'82'	EXTERNAL AUTHENTICATE
'84'	GET CHALLENGE
'88'	INTERNAL AUTHENTICATE
'A4'	SELECT FILE
'B0'	READ BINARY
'B2'	READ RECORD(S)
'C0'	GET RESPONSE
'C2'	ENVELOPE
'CA'	GET DATA
'D0'	WRITE BINARY
'D2'	WRITE RECORD
'D6	UPDATE BINARY
'DA'	PUT DATA
'DC'	UPDATE DATA
'E2'	APPEND RECORD

Table 3 5 Detail Description of INS [4]

P1 and P2: These fields represent the parameters of the function which is mentioned. For example, consider the READ BINARY command. Here the P1 represents file identification parameter and P2 represents the starting parameter of the file which is going to read.

The Response APDU is:

Data	SW1	SW2

Table 3 6 Structure of Response APDU [4]

The Response APDU contains Data, Status words (sw1, sw2). Status word represents the status of the response APDU. Based on the needs of the Sending APDU, the data will be returned.

SW1-SW2	Meaning
'9000'	No further qualification
'6700'	Wrong length
'6B00'	Wrong parameter(s) P1-P2
'6D00'	Instruction code not supported or invalid
'6E00'	Class not supported
'6F00'	No precise diagnosis

Table 3 7 Detail description of Response APDU [4]

4. Design and Implementation

4.1 Design and Implementation of the Server side

4.1.1 Design of the Trusted Service Manager

The Design view of sever part contains two parts. First Part is TSM sever which I mentioned here as mobile application management. This part contains four functionalities. They are List, Update, Customization, and Download. The List functionality provides the List of Applications which is available in TSM server. The Update part displays all the available updates in TSM. The Customization part gives the customized part of individual user application. But Due to the time concern, Download functionality is implemented. Application can be listed and downloaded from the client side (Android).This part includes authentication details to enter inside the functionalities of TSM part.

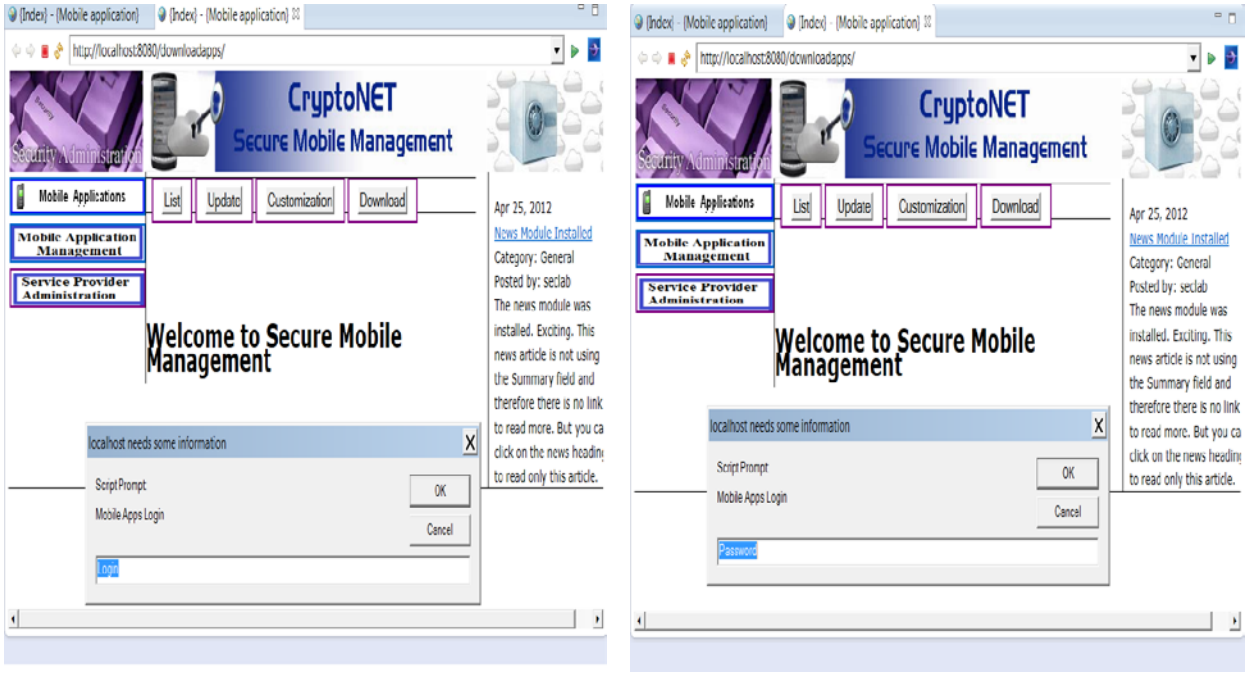

Figure 4 1 Design View of TSM server

4.1.2 Implementation of Trusted Service Manager

The implementation of the server part contains Download function of the application. Tomcat web server has been used as a server. By using the HTTP protocol, the Download functionality has been established. Moreover, the webpage has been created by using Java Sever Pages (JSP) which is used to create dynamic web pages in java environment.

Figure 4 2 Implementation of TSM server

4.1.3 Design view of Service Provider (SP):

The service provider contains five functionalities which are used to do SP administrator's operations. They are Upload, List, Delete, Update, Customization, and Register. Upload part is used to upload the Service Provider's Application by SP. List part displays all the applications which have been uploaded by Service Provider. Register Part includes the Registration for the individual Service Provider. Only the registered Service provider can upload their applications inside the SP admin. Delete part is used to delete the application inside the SP admin. The Update and customization functionalities are same as TSM admin.

Figure 4 3 Design view of service provider

Figure 4 4 Design view of service provider

4.2 Design and Implementation of the Client side

4.2.1 Design View of the Client side:

The design of client side contains two parts. First part defines the design function for android phone which is used to communicate with the TSM server to perform operations like download and personalization. Second part is middleware part which displays command sequences during the communication between android phone and secure micro SD card.

Graphical User Interface for Android Phone to communicate with TSM:

The design of client side contains five parts .They are Download, Personalization Applet, Generate certificate, strong authentication, Key management, Security settings. Download application which is used to download the application from the TSM server. The download application function allows the user to choose their desired application to download from the server. For Example, the available applications are SAFE wallet, PIV applet, EMV wallet, Medical applet .Downloaded application is stored inside the android phone memory (or) external hard drive memory. Then the application will loaded into secure micro SD card from that memory portion. Personalization is used to personalize the application for the individual user. The remaining part is created for to handling the certificate, key management and strong authentication.

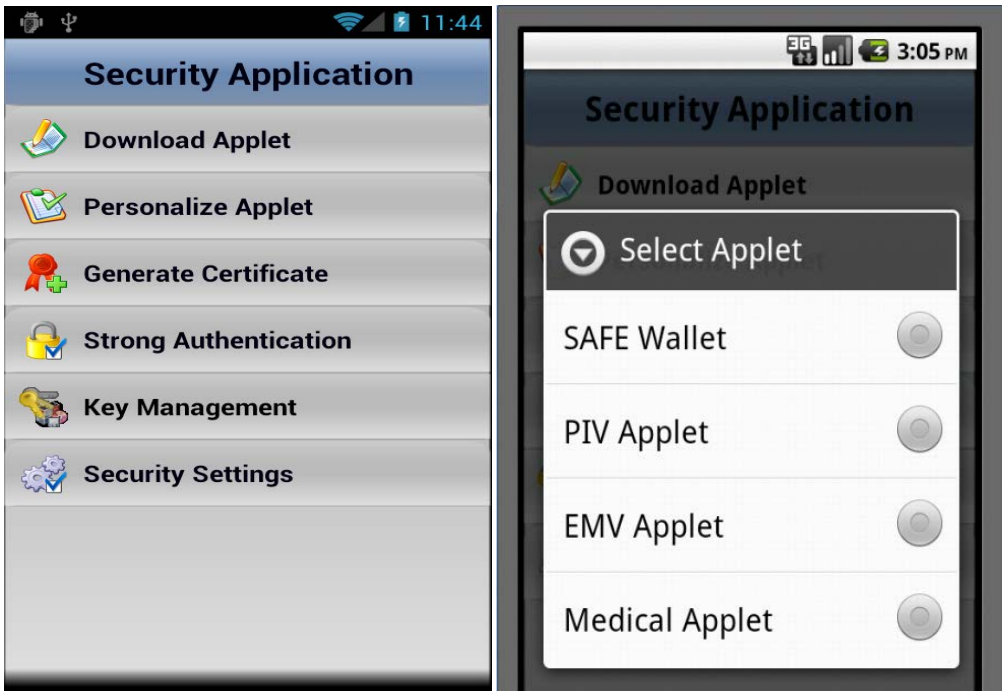

Figure 4 5 Design view of client side

4.2.2 Implementation of Client Side

Implementation of Android part to Communicate with TSM

The Client side implementation contains two parts as discussed in design part of the client. First part is used to download application from TSM server and stored it in External memory of the Android phone. The download function can be done by the HTTP request from the android phone to TSM server. Then the TSM server sends HTTP response based on the request send by android phone.

Figure 4 6 Implementation of Client part with TSM server

4.2.2.1 Implementation of Android middleware to communicate with secure micro SD card

Communication concepts between Android phone and secure micro SD card

The loading applets inside the secure micro SD card can be done only after the download the application inside the Android phone (or) External memory of Android phone. Before load the applet inside the secure micro SD card, the secure channel should be done between android phone and secure micro SD card. Secure Channel means a secure tunnel between the Android mobile and Secure Micro SD card .It remains the mutual authentication between the phone and the Secure Micro SD card. This can be done in two steps. First Step is the creation of session keys. Next Step is establishing the mutual authentication by comparing the Card cryptogram and Host cryptogram. Finally the Mac value has been concatenated with host cryptogram and sends it to card. The successful access of this command means secure channel establishment [8].

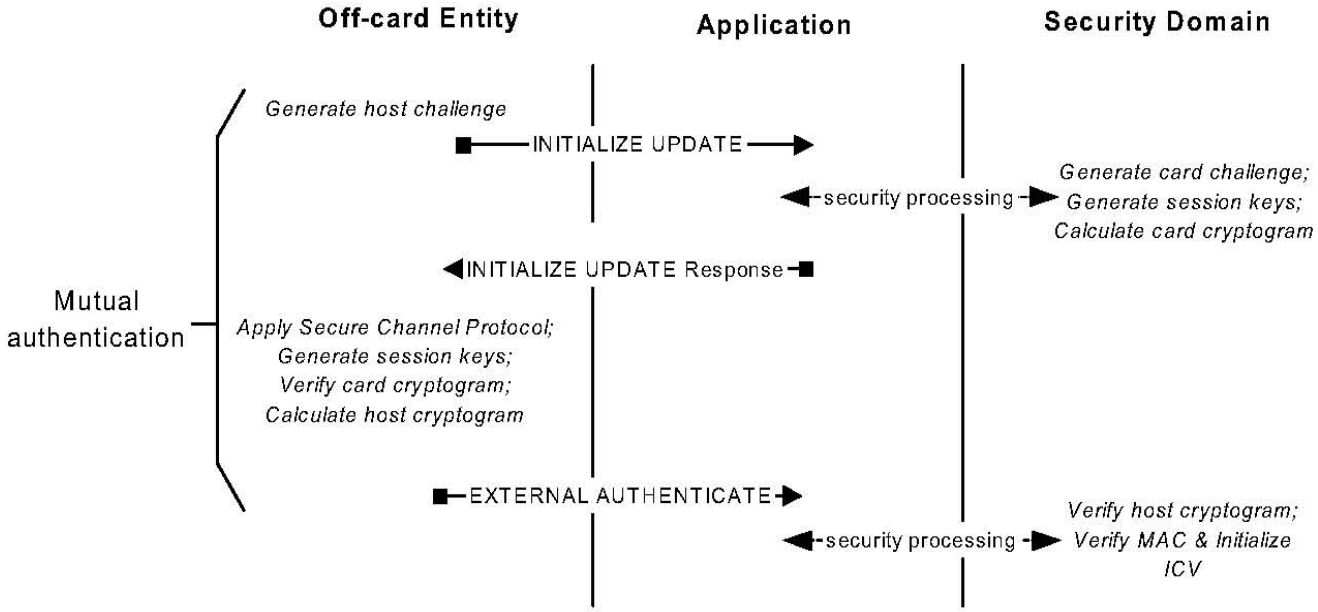

Figure 4 7 Process of secure channel establishment [8]

Creation of Session Keys:

First the Host (android Phone) creates a random block which has 8 bytes and send it to card .this is called host challenge. Then the Secure micro SD card will create 8 bytes random block which is called card challenge. Derivation data (16 bytes) will be created from the host and card challenge. The creation of Derivation data is shown in the figure. Then the Session key is created by using to encrypt the derivation data with static encryption key. 3 DES-ECB algorithms are used for the encryption [8].

Creation of Derivation Data

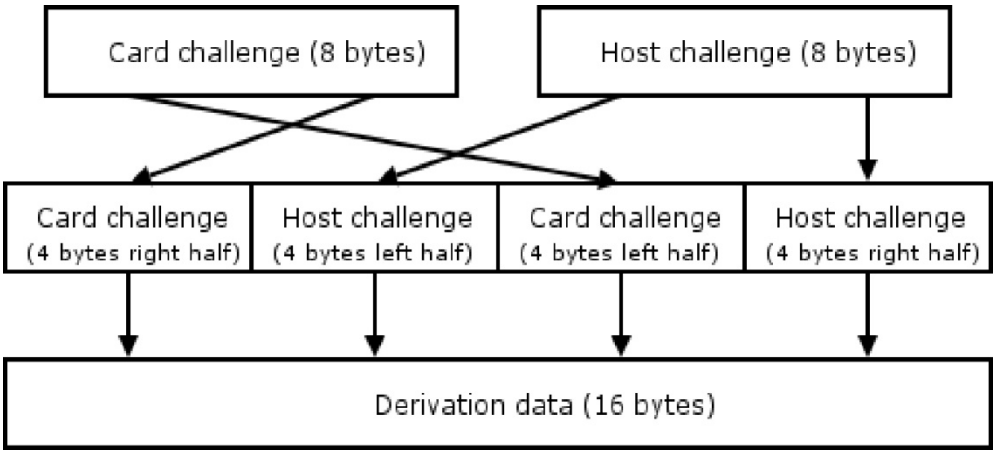

Figure 4 8 Creation of derivation data [8]

Session Key Generation:

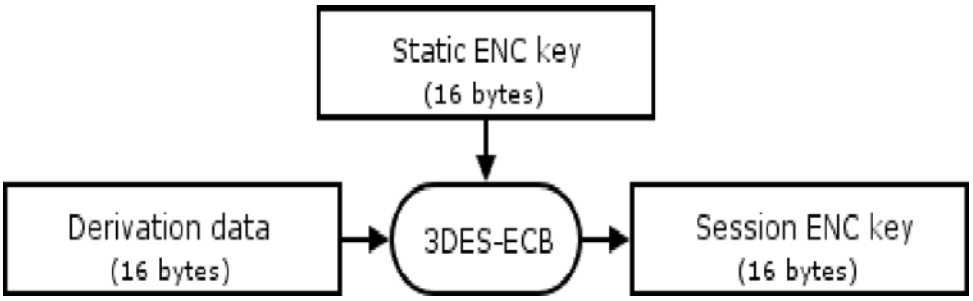

Figure 4 9 Session Key generation [8]

Establishment of secure channel:

The session key is mainly used to create the cryptograms. First the Secure micro SD card cryptogram is created by using the MAC operation. The Card cryptogram is generated by concatenation of the Host and card challenges with the Input Data. Then it is padded by the block (’80 00 00 00 00 00 00 00 ’). The card cryptogram has sent back to android. The android checks that cryptogram and generates its own cryptogram which is called Host cryptogram. If the Card and host Cryptograms are same then the MAC data is concatenated with Host Cryptogram and send it to card by using APDU commands. Host Cryptogram and Card Cryptogram are using the same algorithm. But they are differentiated in placing the Card and host challenges. MAC operations and Session Key encryption are used to create a strong authenticated secure tunneling between the secure micro SD card and the Android phone [8].

MAC Computational Algorithm

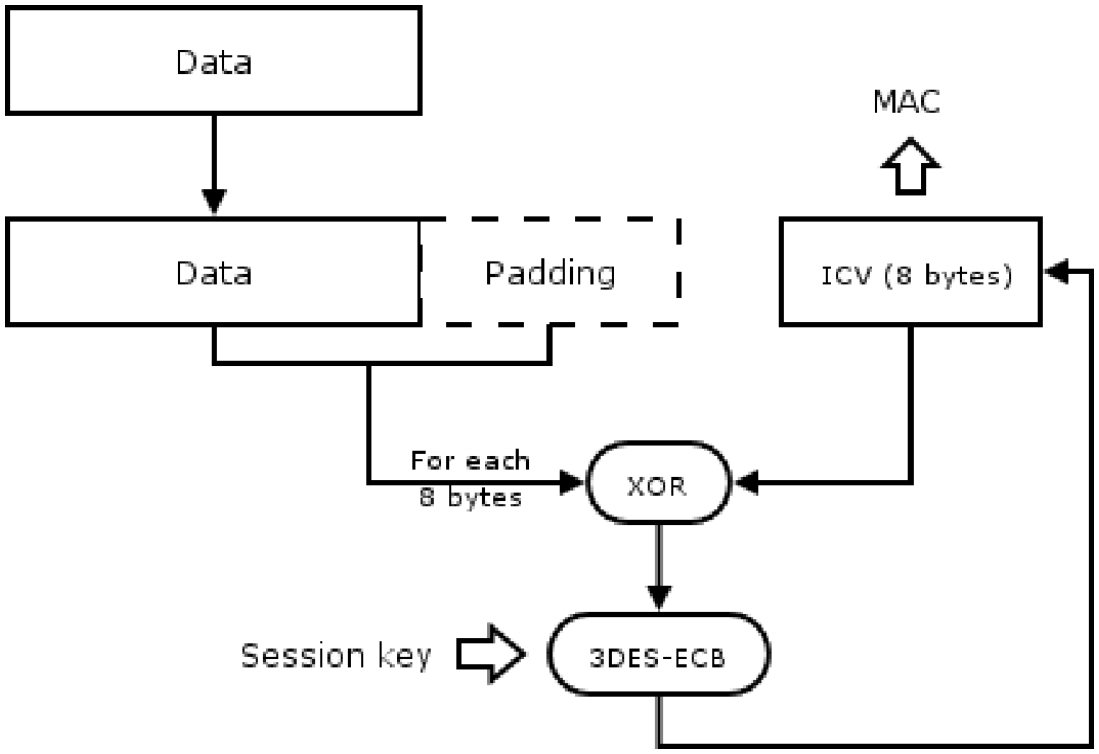

Figure 4 10 MAC computational Algorithm [8]

Java Security Libraries:

Bouncy Castle java crypto libraries are used to do the crypto graphic operations. This research two places that are needed to do some crypto functions. They are session key generation and MAC computation (figures no). Here Triple DES- ECB mode cryptographic algorithms are used for the encryption and decryption of the data. Bouncy castle API's are useful to utilize the Triple DES algorithm in Single line of code. If not a large number of codes need to be written to implement the Triple DES algorithm.

Android SDK:

Software Development Kit is used to develop some applications on operating system of android .This kit supports java platform which is very useful to load java libraries, Crypto libraries and secure micro SD card's API. The tutorial for android SDK is available on Internet which gives some guidelines to develop applications on Android phone.

Secure Micro SD card API's

Secure micro SD card API is the instruction which is used to communicate the Android phone with the secure micro SD card. There are lot of PI has been mentioned in Oberthur Secure micro

SD card developer guide. This Research uses the below APIs to communicate with the secure micro SD card. They are

Card Initialization:

This is the Starting step before using the Secure Micro SD card operations. It Initialize the settings of Secure Micro SD card.

Syntax:

Char ReturnValue= OT_SmartSD card_Initialization(String SDcard Path) [1];

If the Return Value is 0 then the APDU request has been successfully accessed by the secure micro SD card. If not means Failure message.

Card Reset:

This APDU command is used to send the APDU request to reset the secure micro SD card.

Syntax:

Char Return Value= OT_SmartSDcard_reset(int ATR length[],char[] ATR Buffer) [1];

If the Return Value is 0 then the APDU request has been successfully accessed by the secure micro SD card. If not means Failure message

Smart Card Access APDU command:

This command is used to send APDU request to Secure Micro SD card and get APDU response from the Secure Micro SD card.

Syntax;

Char ReturnValue=OT_smartSDcard_AccessAPDU Command (int sendAPDU length, char[] sendAPDUBuffer,int GetAPDUlength,char[] GetAPDUBuffer,int waitingtime) [1];

If the Return Value is 0 then the APDU request has been successfully accessed by the secure micro SD card. If not means Failure message

4.2.2.2 Implementation of secure channel and load applet inside the secure micro SD card:

First the user is allowed to choose the application which he wants to load inside the secure micro SD card. Figure 4 11 Shows the List of applets which can select by the user. For Example, the applications which are stored inside the External memory from the TSM server. Secure channel should be established before load applet inside the secure micro SD card.

Secure channel Establishment:

After selection of the particular application, the card initialization has been processed by using the secure micro SD card APIs. Then secure micro SD card reset has been performed. Then First Step of secure channel establishment is initialization update. The host (android phone) sends some challenges to secure micro SD card which is called Host challenge. The host challenge contains 8 bytes. Secure micro SD card return some data. The successful return data should return the card challenge and card cryptogram. Then the Host will generate the session key and find its Host cryptogram. Figure 4 11 shows secure micro SD card return value under the Initialize update headline. It has 9000 APDU at the end which means the sending APDU is successfully accessed by secure micro SD card and the return data is also correct. The APDU

response contains card challenge and also card cryptogram. Then the host cryptogram has been generated.

Figure 4 11 & 4 12 shows card cryptogram and host cryptogram also same. So the card and Host cryptogram has been combined with MAC value and send it card. This method is External authenticate. Figure 3 shows the External authenticate method under Establishing secure channel headline. The card returns 9000. So it means the two function initialization update and External authenticate have been done successfully which means secure channel has been established.

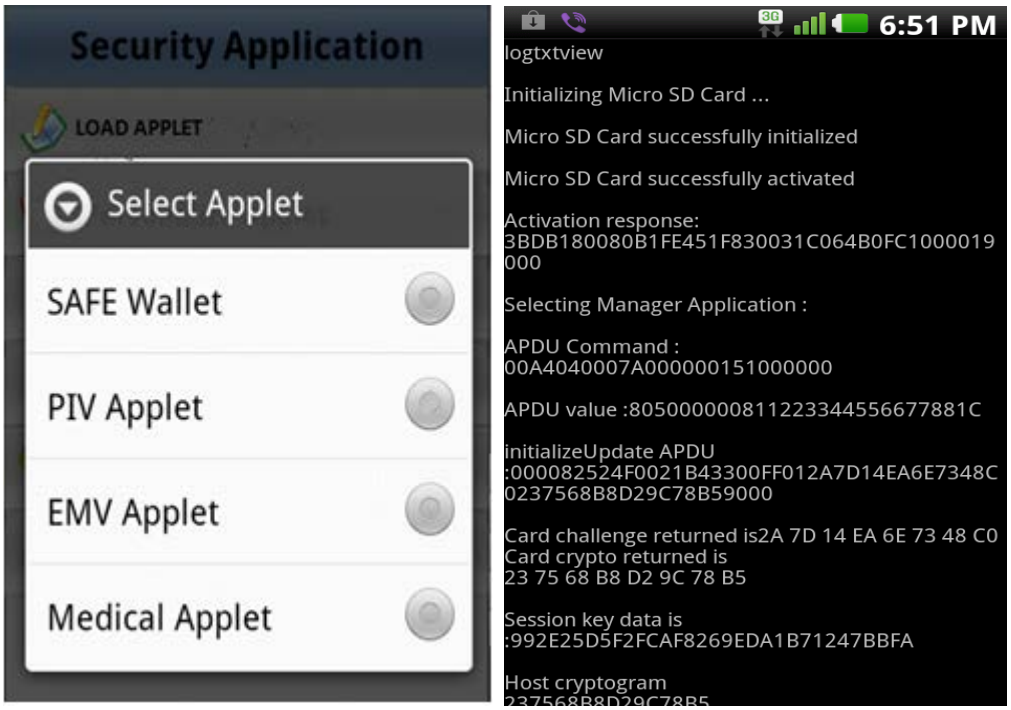

Figure 4 11 Selection of an Applet and generation of cryptograms

Load Applet:

After Establishment of secure channel, we can perform load applet inside the secure micro SD card. Because secure channel gives the mutual authentication between the android phone and secure micro SD card. But the Figure 4 12 shows delete applet after establishing secure channel. Because the secure micro SD card already have an applet inside. As discussed earlier, the secure SD card cannot able to store multiple applications. So, delete applet can be performed before load applet. Figure 4 12 explains procedure of loading applets. For that, the applet path should be mentioned. Not only the path but also the applet size, Applet ID and Program file ID. So that, the secure micro SD card can read the data and loaded inside the secure micro SD card. The load applet can be mentioned in Figure 4 13& 4 14. Here the wallet application has been loaded inside the secure micro SD card. Then finally wallet application can be selected by using the Select applet method which can be described in Figure 4 14and also verify the applet pin.

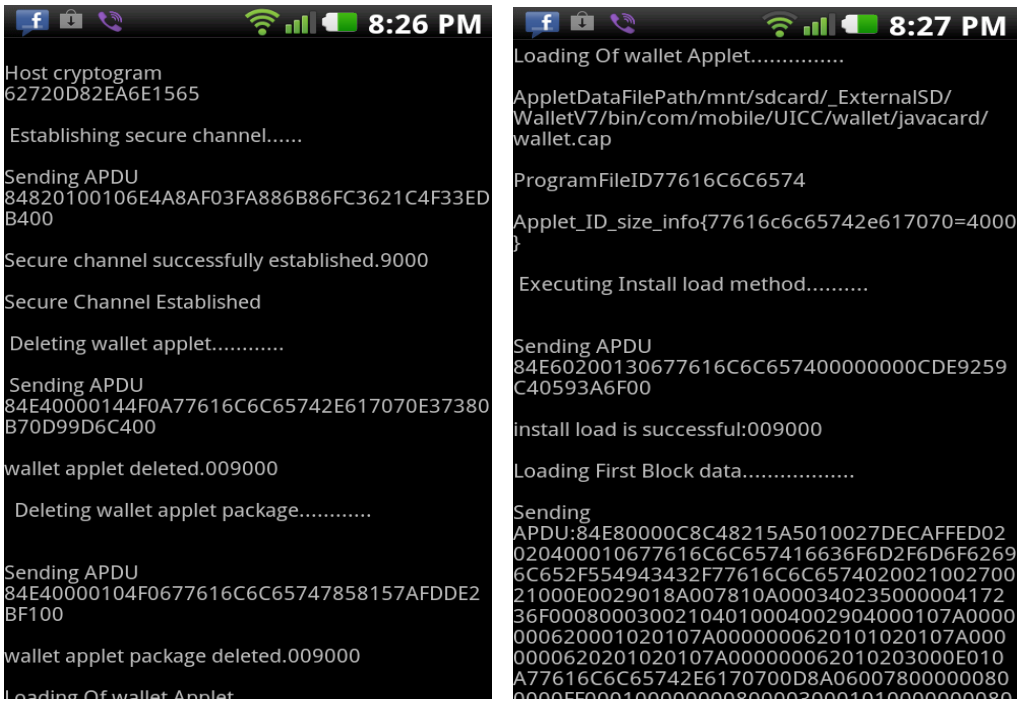

Figure 4 12 Establishment of secure channel and load first block data

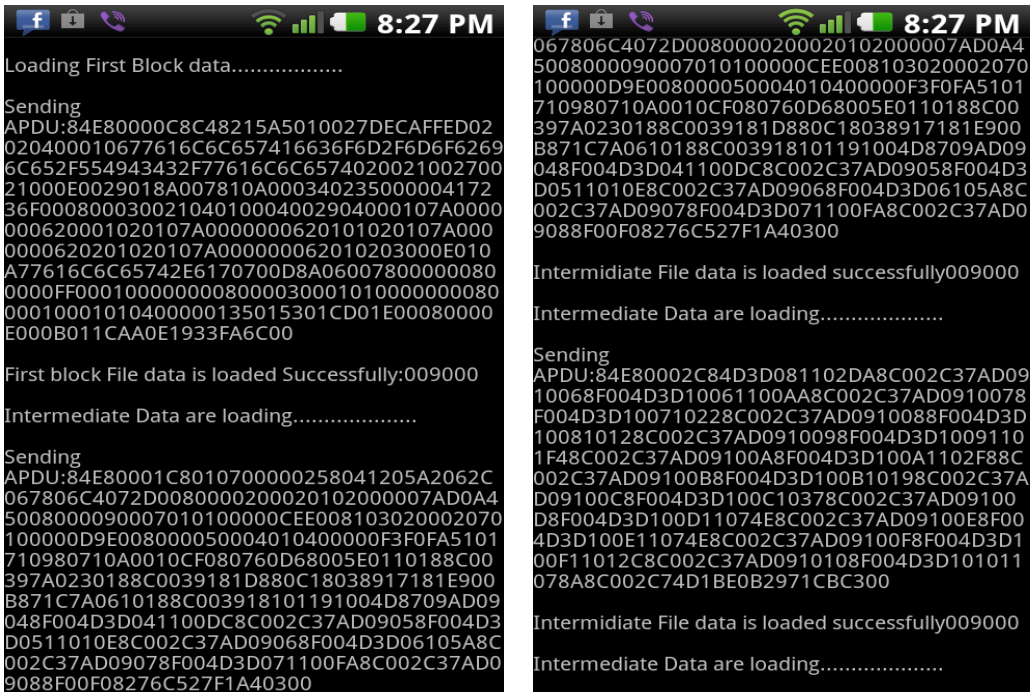

Figure 4 13 Load intermediate block of data

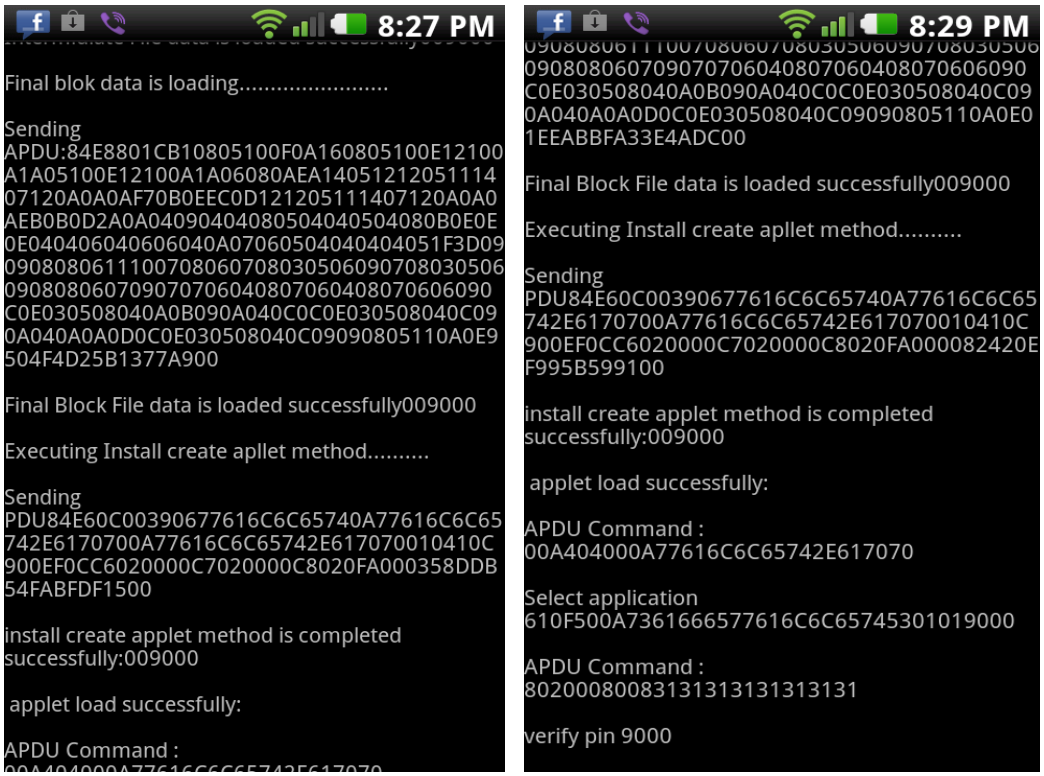

Figure 4 14 Load the Final block data and verify the applet inside the card

5. Conclusions and Future Work

5.1 Conclusions

This research finds the solution to store the application in over the air mobile application management. As the result of this research, a prototype has been implemented for storing the application inside the secure micro SD card. The prototype has been implemented by using the ISO 7816-4 Standard. This is the main goal of this thesis which has been implemented.

The two sub goals of this research also have been implemented. The sub goals are

- Established Secure OTA provisioning between the TSM and Android (Communicator with Secure micro SD card).
- Established the Secure OTA provisioning between Android and Secure micro SD card.

The sub goals of this research have implemented by implementing some functions. The functions are,

- Constructed the Design of Trusted Service Manager (TSM) and Service provider.
- Implemented the Functionality of TSM Server (Download Function) and tested the Functionality whether the end terminal (Android Phone) has been able to use the function properly.
- Established the secure channel between the Android phone and secure micro SD card.
  It contains below steps.
  - Generation of Host and Card challenges.
  - Creation of session Keys.
  - Calculation of Card and Host cryptograms.
  - Secure channel establishment by using MAC operation.
- Tested the secure channel establishment by verifying APDU commands. (Example) If the card returns APDU response 9000, the Command which has been send by Android has been successfully accessed by the card.
- Loaded the sample application inside the secure micro SD card and test the presence of the application inside the card.

5.2 Future Work

The research has lot of works which provide the complete security. They are

- Implement the remaining functionalities of the TSM server. (Example) list of the applications, Customization, Update.
- Implement the remaining functionalities of service provider. (Example) Update the new application, Delete the application.
- Personalize the application which is stored inside the micro SD card.
- In the client side, establish strong authentication by generate certificates.

6. References

1.Card, O. (2012, May 20). Software development guide for oberthur micro SD card.

2. *Card-payments*. (n.d.). Retrieved Augest 23, 2012, from Financial-news: http://www.vrl-financial-news.com/cards--payments/cards-international/issues/ci-2011/ci-463-464/sim-vs-sd-under-the-skin-of-n.aspx

3. gemalto. (n.d.). *tsm*. Retrieved June 13, 2012, from gemalto: http://www.gemalto.com/nfc/tsm.html

4. Hao, Z. (2011., May 17). Integrated secure platform for mobile applications. 114.

5. J.cronin, S. B. *Mobile Appilcation Development with SMS and SIM toolkit.* New York, United States of America: Mcgraw-hil.

6. jools, c. (n.d.). OTA and secure SIM lifecycle Management. 19.

7. *ota-over-air-provisioning*. (2009, November). Retrieved May 11, 2012, from computingtechnologies: http://computingtechnologies.blogspot.se/2009/11/ota-over-air-provisioning.html

8. Platform, G. (n.d.). *SC_SecureMessaging*. Retrieved April 12, 2012, from Global Platform: http://www.fi.muni.cz/~xsvenda/docs/SC_SecureMessaging.pdf

9. secure_elements_solutions. (n.d.). *secure_elements_solutions*. Retrieved June 15, 2012, from windblazer: http://www.windblazer.pe.kr/wordpress/wpcontent/uploads/2011/03/secure_elements_solutions.jpg

10. *servlet*. (n.d.). Retrieved May 24, 2012, from frost: http://www.frost.com/prod/servlet/cio/188029279

11. Technologies, S. P. (n.d.). Retrieved July 11, 2012, from http://www.google.se/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&cad=rja&ved=0CFIQFjAI&url=http%3A%2F%2Fwww.sptek.com%2Feng%2Fdown%2Fdown.asp%3FFCode%3D10&ei=DYRhUJjRIIWi4gS_Mw&usg=AFQjCNEj7bq-LWdQvCnLBbr_oIzy320sUw

12. Hao Zhao, Sead Muftic, Feng Zhang, “The Secure Mobile Wallet”, Cutter IT Journal, July 2010, Page 32~35

13. gemalto. (n.d.). *ota*. Retrieved May 23, 2012, from gemalto:http://www.gemalto.com/techno/ota/

14.Gemplus, O. S. (2003, October 6). *WG3 security*. Retrieved June 22, 2012, from 3gpp: http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_30_Povoa/Docs/PDF/S3-030534.pdf

15. solutions, c. (n.d.). *OTA solutions*. Retrieved Augest 25, 2012, from commverge: http://www.commverge.com/Solutions/SubscribersServicesManagement/OverTheAirOTASolutions/tabid/176/Default.aspx