

*Master Thesis*  
*Electrical Engineering*  
*Thesis no: MSSEE-2010-26011*  
*June, 2011*



# **Secure Identification in Social Wireless Networks**

**Omer Nawaz**

School of Computing  
Blekinge Institute of Technology  
SE – 371 79 Karlskrona,  
Sweden

This thesis is submitted to the School of Engineering at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Electrical Engineering. The thesis is equivalent to 20 weeks of full time studies.

**Contact Information:**

Author: Omer Nawaz

E-mail: omna09@gmail.com

**External Advisor:**

Christian Gehrman, Ph.D.

Secure Systems Group

Swedish Institute of Computer Science (SICS)

Address: Scheelevägen 17, 223 70 Lund, Sweden

Phone: +46 76 881 3690

**University Advisor:**

Markus Fiedler, Ph.D.

School of Computing

Blekinge Institute of Technology

SE – 371 79 Karlskrona.

Phone: +46 455 385 653

**University Examiner:**

Patrik Arlos, Ph.D.

School of Computing

Blekinge Institute of Technology

SE – 371 79 Karlskrona.

Phone: +46 455 385 444

School of Computing  
Blekinge Institute of Technology  
SE – 371 79 Karlskrona  
Sweden

Internet : [www.bth.se/com](http://www.bth.se/com)  
Phone : +46 457 38 50 00  
Fax : + 46 457 271 25

## **ABSTRACT**

The applications based on social networking have brought revolution towards social life and are continuously gaining popularity among the Internet users. Due to the advanced computational resources offered by the innovative hardware and nominal subscriber charges of network operators, most of the online social networks are transforming into the mobile domain by offering exciting applications and games exclusively designed for users on the go. Moreover, the mobile devices are considered more personal as compared to their desktop rivals, so there is a tendency among the mobile users to store sensitive data like contacts, passwords, bank account details, updated calendar entries with key dates and personal notes on their devices.

The Project Social Wireless Network Secure Identification (SWIN) is carried out at Swedish Institute of Computer Science (SICS) to explore the practicality of providing the secure mobile social networking portal with advanced security features to tackle potential security threats by extending the existing methods with more innovative security technologies. In addition to the extensive background study and the determination of marketable use-cases with their corresponding security requirements, this thesis proposes a secure identification design to satisfy the security dimensions for both online and offline peers. We have implemented an initial prototype using PHP Socket and OpenSSL library to simulate the secure identification procedure based on the proposed design. The design is in compliance with 3GPP's Generic Authentication Architecture (GAA) and our implementation has demonstrated the flexibility of the solution to be applied independently for the applications requiring secure identification. Finally, the thesis provides strong foundation for the advanced implementation on mobile platform in future.

**Keywords:** Secure Identification, Internet Security, GBA, UICC

## **ACKNOWLEDGEMENTS**

First of all, thanks to Almighty, the most beneficial and merciful. It was not possible without blessings of The Creator and his Messenger (PBUH).

I would especially like to gratitude Mr. Christian Gehrmann for intense efforts and support in terms of resources and thorough guidance within this study. He really pushed and strengthened me whenever I get lost during the work. Furthermore, salute to his patience during the later part of this project.

This thesis would never have been completed without the help of Mr. Markus Fiedler who always backed by reinforcing trust and motivated me throughout this study.

Finally, dedication to my parents and family, especially to my mother who remains source of intuition for me and who always sacrificed for the further studies of her children. Thanks Dad for your encouragement and financial support in all my endeavors.

# TABLE OF CONTENTS

<b>ABSTRACT .....</b>	<b>I</b>
<b>ACKNOWLEDGEMENTS .....</b>	<b>2</b>
<b>TABLE OF CONTENTS .....</b>	<b>3</b>
<b>LIST OF FIGURES.....</b>	<b>5</b>
<b>ABBREVIATIONS.....</b>	<b>7</b>
<b>1 INTRODUCTION .....</b>	<b>9</b>
1.1 PROJECT SWIN.....	10
1.2 THESIS ORGANIZATION.....	10
1.3 PROBLEM DEFINITION.....	10
1.3.1 Originality.....	11
1.3.2 Scope of the thesis.....	11
1.3.3 Research Questions.....	11
1.4 AIMS AND OBJECTIVES .....	12
1.5 RESEARCH METHODOLOGY .....	12
<b>2 SECURE IDENTIFICATION.....</b>	<b>13</b>
2.1 USE-CASES .....	13
2.1.1 Fashion Industry.....	13
2.1.2 Religious Factions .....	14
2.1.3 Business Network.....	15
2.2 USE CASE ANALYSIS .....	16
2.2.1 Business aspect .....	16
2.2.2 Technological aspect .....	18
2.3 SECURITY REQUIREMENTS.....	20
2.3.1 Secure Registration and Authentication .....	20
2.3.2 Profiles and Location Based Services.....	21
2.3.3 Access Control and Data Storage.....	21
2.3.4 Managing real-time services.....	21
2.4 SUMMARY.....	22
<b>3 STATE OF THE ART.....</b>	<b>23</b>
3.1 MOBILE SOCIAL NETWORKS .....	23
3.1.1 Online Social Networks .....	23
3.1.2 Social Networks in Mobile Domain.....	24
3.2 SECURE IDENTIFICATION SCHEMES.....	26
3.2.1 Secure routing schemes in Ad hoc networks using PKI.....	26
3.2.2 Symmetric and Layered approaches.....	26
3.2.3 Location Anonymity .....	28
3.3 KEY EXCHANGE SCHEMES.....	29
3.3.1 Secure Identity Management and Sharing .....	29
3.3.2 Generic Authentication Architecture .....	31
3.3.3 Generic Bootstrapping Architecture (GBA) .....	32
3.3.4 Support for subscriber certificates (SSC) .....	34
3.3.5 SPKI and SDSI.....	36
3.3.6 Device Pairing .....	36
3.3.7 Manual Authentication Using MAC (MANA III) .....	37
3.4 TRANSPORT LAYER SECURITY (TLS) .....	38
3.4.1 TLS Handshake Protocol.....	39
3.4.2 TLS Change Cipher Specs (CCS) .....	40
3.4.3 TLS Alert Protocol.....	40

3.4.4	<i>TLS Record Protocol</i> .....	41
3.5	SUMMARY .....	41
<b>4</b>	<b>SECURE IDENTIFICATION DESIGN</b> .....	<b>42</b>
4.1	ARCHITECTURE OVERVIEW .....	42
4.1.1	<i>Certificate Structure</i> .....	43
4.1.2	<i>Database Model</i> .....	43
4.2	NETWORKING ELEMENTS AND REQUIREMENTS .....	44
4.2.1	<i>User Equipment</i> .....	44
4.2.2	<i>Bootstrapping server function (BSF)</i> .....	45
4.2.3	<i>PKI</i> .....	45
4.2.4	<i>MSNP</i> .....	45
4.2.5	<i>Reference point Zsn</i> .....	46
4.2.6	<i>Reference point Ub andUa</i> .....	46
4.2.7	<i>Reference point Usn</i> .....	46
4.3	KEY EXCHANGE SCHEME .....	46
4.3.1	<i>User Certificate Enrollment</i> .....	47
4.3.2	<i>New registration and creation of new social group</i> .....	47
4.3.3	<i>Secure authentication of registered users</i> .....	49
4.3.4	<i>Online invitation to new members</i> .....	50
4.3.5	<i>Joining procedure for user invited in online mode</i> .....	51
4.3.6	<i>New group creation by already registered members</i> .....	52
4.4	SECURE IDENTIFICATION IN OFFLINE MODE .....	52
4.4.1	<i>Offline invitation by moderator to non-registered user of group</i> .....	52
4.4.2	<i>Offline authentication of users belonging to same group</i> .....	54
4.5	SUMMARY .....	54
<b>5</b>	<b>PROTOTYPE IMPLEMENTATION</b> .....	<b>55</b>
5.1	PROTOTYPE STRUCTURE .....	55
5.1.1	<i>Prototype Platform</i> .....	55
5.1.2	<i>Prototype Architecture</i> .....	56
5.2	SOFTWARE MODULES .....	56
5.2.1	<i>PHP Sockets</i> .....	56
5.2.2	<i>PHP OpenSSL Module</i> .....	56
5.3	SECURITY ANALYSIS .....	57
5.3.1	<i>Secure Connectivity</i> .....	57
5.3.2	<i>Potential Attack</i> .....	57
5.4	MSNP PROTOTYPE RECOMMENDATIONS .....	57
5.4.1	<i>Server Mode</i> .....	57
5.4.2	<i>Client Mode</i> .....	58
5.5	DEMONSTRATION .....	59
5.5.1	<i>Secure Registration</i> .....	59
5.5.2	<i>New Social Group and Online Invitation</i> .....	59
5.5.3	<i>Offline Authentication and Invitation</i> .....	61
5.6	SUMMARY .....	62
<b>6</b>	<b>CONCLUSION AND FUTURE WORK</b> .....	<b>63</b>
6.1	CONCLUSION .....	63
6.2	FUTURE WORK .....	64
	<b>APPENDIX A</b> .....	<b>65</b>
	<b>BIBLIOGRAPHY</b> .....	<b>75</b>

## LIST OF FIGURES

Fig. 1: Use Case diagram of business network .....	19
Fig. 2: Kerberos version 5 based authentication scenario [31] .....	27
Fig. 3: OpenID Authentication flow .....	30
Fig. 4: GAA Architecture.....	31
Fig. 5: GBA network model with application server outside internal network [6]....	32
Fig. 6: Bootstrapping procedure [6] .....	33
Fig. 7: Reference model for issuance of certificates [42] .....	34
Fig. 8: Message flow for issuing certificate [42] .....	35
Fig. 9: Device pairing using user verification scheme [48] .....	36
Fig. 10: Manual authentication using MAC [47] .....	38
Fig. 11: TLS Protocol Stack [49] .....	38
Fig. 12: TLS Handshake Protocol [49] .....	40
Fig. 13: Simple model for mobile social network portal .....	42
Fig. 14: Database model for MSNP secure identification module.....	43
Fig. 15: New user registration flow.....	48
Fig. 16: Online invitation flow initiated by moderator .....	50
Fig. 17: Offline authentication procedure for non-registered users of particular group .....	53
Fig. 18: Prototype Architecture.....	56
Figure A. 1: Home screen of thesis prototype .....	65
Figure A. 2: Generation of key pairs and certificates signing requests .....	65
Figure A. 3: Download page for generated credentials .....	66
Figure A. 4: Validating certificate request .....	66
Figure A. 5: New user registration .....	67
Figure A. 6: Validating certificates and server key after secure registration.....	67
Figure A. 7: Sign in page for registered user.....	68
Figure A. 8: View via download option of server public key.....	68
Figure A. 9: Page view after successful login .....	69
Figure A. 10: Page for creation of new social group.....	69
Figure A. 11: Online invitation page .....	70
Figure A. 12: Inviting another user to your social group.....	70
Figure A. 13: Validating online invitation request .....	71
Figure A. 14: Creating offline connection via sockets .....	71

Figure A. 15: Validation of random numbers and sent vector via ViDP protocol .....72

Figure A. 16: Validation of received certificate and invitation vector by other user .....72

Figure A. 17: Invitation vector in encrypted form.....73

Figure A. 18: Getting online and joining social group via offline invitation .....73

Figure A. 19: Successful membership via credentials received in offline mode.....74

## **ABBREVIATIONS**

AKA	Authentication and Key Agreement
AP	Authentication Proxy
API	Application Programming Interface
AS	Authentication Server
AUTH-1	Authenticator
BSF	Bootstrapping Server Function
CA	Certificate Authority
CSR	Certificate Signing Request
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GBA_ME	ME-based GBA
GBA_U	GBA with UICC-based enhancements
GUSS	GBA User Security Settings
HSS	Home Subscriber System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
LBS	Location Based Services
MNO	Mobile Network Operator
MSNP	Mobile Social Networking Portal
NAF	Network Application Server
NE	Network Element
OP	OpenID Provider
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
RP	Relaying Party
SA	Security Association
SSC	Support for Subscriber Certificates
SSO	Single Sign-On Service
TGS	Ticket Granting Server
TLS	Transport Layer Security
UE	User Equipment

UICC	Universal Integrated Circuit Card
URL	Uniform Resource Locator
USS	User Security Setting
VIP	Verisign Identity Protection
3GPP	3 <sup>rd</sup> Generation Partnership Project

# 1 INTRODUCTION

Online social networking has brought revolution towards social life by facilitating interaction with old friends, sharing of events, distribution of data and various other aspects of social life. Due to the advanced computational resources offered by innovative hardware and nominal subscriber charges of the network operators, there has been an emerging trend among subscribers to access web-based services via mobile devices. The latest mobile based software also support ease of personalization as compared to their desktop rivals like change of language, settings etc. As a consequence, most of the popular social networking websites are transforming into mobile domain by offering exciting applications and games exclusively designed for users on the go. Some of these services include maps and Location Based Services (LBS) that influence the anonymity and privacy of users. There have been continuous doubts related to security concerns emerging due to the leakage of confidential data, copyrights violation, privacy of individual etc. Moreover there is a tendency among users to store private and sensitive data on their mobile phones as compared to typical personal computer like contacts, passwords, bank account details, updated calendar entries with key dates and personal notes. Hence, the situation arises to be a tradeoff among these exciting features and consequence security threats.

As mobile communications are considered to be fairly safe and trusted by end-users, thus incorporating social networks should not compromise the attained security levels and avoid risks incorporated at internet level [1]. The success of any mobile social network primarily depends on its security based dimensions which includes secure registration and authentication, integrity control and privacy protection.

Most of the traditional services running on mobile phones require authentication and Generic Authentication Architecture (GAA) is a 3GPP's solution which help users to avoid manual management of credentials to access those services [2]. The GAA supports two different kinds of authentication mechanisms where the first rely on pre-shared secrets and the later use public, private key pairs and corresponding digital certificates to manage the authentication requirements of various applications [3].

The current thesis is a part of the Research and Development (R&D) project carried out at SICS in collaboration of Sony Ericsson [1]. It is an effort to probe and improve the existing key-exchange mechanisms for USIM, ISIM environments [4] to provide secure identification in mobile social networks. The solution provides secure authentication between the client and Mobile Social Networking Portal (MSNP). The prime focus for this particular thesis is to manage the secure communication between two mobile peers (Offline Mode) along with secure invitation from user of either network using novel key exchange mechanism by avoiding complete re-authentication procedure. The solution is based on public, private key pairs and

corresponding authentication, signing and social certificates managed by the Mobile Network Operator (MNO). The registration, invitation and offline invitation process is emulated by implementing a prototype. Finally, preliminary security analysis is carried out for verification of the prototype.

## **1.1 Project SWIN**

The Project Social Wireless Network Secure Identification (SWIN) [1] is carried out at Swedish Institute of Computer Science (SICS) in collaboration with Sony Ericsson Lund and Ericsson AB Stockholm. According to the basic guidelines available at [1], the project is intended to enhance current mobile security standards with a possible extension to incorporate the challenging security requirements of mobile based social networking portals. The project is carried out in three dimensions:

- Authentication
- Android Security
- Privacy in Mobile Social Networks

This particular thesis is primarily targeting the authentication part of the project. The potential problems that are related to privacy in mobile social networks like location based services and identity management are also probed at an abstract level.

## **1.2 Thesis Organization**

Chapter 1 provides the basic introduction. Chapter 2 and Chapter 3 cover the scope of the complete SWIN [1] project. Hence, these chapters cater the security requirements and literature summary related to the Mobile Social Network Portal (MSNP). Some of the potential use-cases along with their business and technological aspects are discussed in Chapter 2. This chapter also defines the security requirements for successful realization of the MSNP. Chapter 3 summarizes the research work done in the targeted domains related to MSNP and their brief summary. Chapter 4 illustrates the proposed solution only for the secure identification procedure in MSNP. Chapter 5 covers the prototype implementation for this particular thesis. Chapter 6 remarks the conclusion and brief guideline for future work.

## **1.3 Problem Definition**

The exciting features offered by existing mobile based social networks arise at a cost of privacy protection and anonymity disclosure. Decentralized online social networks are gaining popularity and transforming this phenomenon into mobile domain comprises additional security challenges. Therefore, the security challenges that needed to be tailored within this thesis can be summarized as:

- Strong authentication procedures for eradicating both active and passive threats.
- Authorized client should register new members in offline mode.
- Confidentiality and Integrity on the non-trusted media and collaboration with open compromised networks.
- The solution should be in compliance with current GAA [3] standards.

### **1.3.1 Originality**

Although the mobile bootstrapping technologies are targets of ongoing research activities but significant amount of work is needed for satisfying the security requirements of mobile social networks. Moreover, the concept of closed networks in mobile environment with exciting opportunities for offline communications is a novel idea. The prime reason for this situation is the fact that application authentication is considered out of the scope when it comes to GAA [3]<sup>1</sup>. Furthermore, targeting secure identification by focusing on the security requirements of decentralized mobile social networks is a quite new research domain.

### **1.3.2 Scope of the thesis**

The scope of this thesis can primarily be categorized into two dimensions:

1. The analysis and design which includes background study, identifying marketable use-cases, determining the security requirements, state of the art, middle ware architectural solution, targets the complete SWIN project.
2. Besides that, the proposed design is validated through prototype implementations of server and client in this study, the main theme is to investigate and propose secure identification and key exchange mechanisms. The solution is able to withstand between online users and USIM based online and offline (direct mode) users.

### **1.3.3 Research Questions**

Based on the problem definition described above, the following research questions were identified to be answered within this study:

- **RQ1:** What would be the futuristic popularity trends of mobile based online social networks?
  - **SQ1.1:** Are there any potential use cases for de-centralized social networks or closed user groups?
- **RQ2:** How can existing boot strapping and key-exchange mechanisms (GAA) can be extended to support secure authentication and accomplish security associations that would provide authentication and privacy protection?

---

<sup>1</sup> Please refer to Page 13 of 3GPP TS 33.919 (GAA Architecture)

- **RQ3:** Would the proposed solution be able to dynamically incorporate mutual authentication simultaneously in both online and direct (offline) mode of operations?
- **RQ4:** How the solution would be flexible to be applied independently by using its key-exchange mechanism without SIM/USIM (GBA) based key-exchange standards for providing autonomous security services?

## **1.4 Aims and objectives**

- Analysis of current online and mobile based social networking solutions.
- Predicting futuristic trends and identifying marketable use cases and the related security requirements.
- Analysis of Boot Strapping and Key-exchange mechanisms [5, 6].
- Identifying the limitations of current Generic Bootstrapping Architecture (GBA) [6] standard to support closed mobile social networks.
- Identifying problems and short comings of current GBA [6] authentication and key exchange mechanism to handle direct mode of communication.
- Proposing design for secure identification.
- Prototype implementation of the proposed design.
- Report

## **1.5 Research Methodology**

The research is primarily based on the principle of induction and deduction. The research questions were carefully identified and then the solution was proposed to fulfill all the identified requirements. The intensive background study and proposed solution guided towards the prototype implementation. The results obtained from the implementation motivates for future work based on the deductive approach.

## **2        SECURE IDENTIFICATION**

Secure identification in terms of network security can be classified into various dimensions, which may comprise secure authentication, integrity control and privacy protection. Secure identification can provide revolutionary trend towards social networking, especially when extended to wireless or cellular networks domain. In this chapter, we will discuss some potential use-cases along with their analysis from business and technological point of view. Finally, we will discuss the minimal security requirements that are necessary to make these use cases realized into a workable solution.

### **2.1      Use-Cases**

The services offered by existing online social networks revolutionized the existing social trends by providing online users a chance to share ideas with friends, friends of friends or even with those they don't know altogether. The extension of current online social networks into the mobile domain provide light weight versions accessible by mobile handsets having internet accessibility and some features like short messaging notifications etc.

Although, whether the existing online social networks would be able to sustain continuing popularity is a highly debatable issue but there is an agreement in broader sense that the current open trend would be shifted towards closed user groups in the coming decade [13]. Some of these closed user groups are identified as use cases for this particular study from various alternative scenarios. The list is as follows:

- Fashion Industry
- Religious Factions
- Business Network

The particular set of functionality required for these use-cases is briefly explained below

#### **2.1.1    *Fashion Industry***

This group should be dedicated to the modeling companies that arrange events related to fashion industry i.e. fashion shows, concerts, photo-shots, advertisements, social gatherings etc.

Suppose a medium sized modeling company that is hiring staff comprising of managers, marketing personals, dress designers, choreographer's, beauticians, photographers, models, office staff etc. The company works in close co-operation with certain media groups and enterprises for marketing their products and arranges various events and fashion shows funded by enterprises.

Now the company would certainly like to have a secure mobile based social network which can become the backbone for its operations. Moreover the company would be working with various dress designers, beauticians, photographers around the globe based on the location of its next event. The prime focus of the event manager is to make sure that everything is perfect and every person involved should be aware of its role prior to the event.

The portal will help the event manager for announcements and description of event, status and availability of models etc for specific events that are held overseas, post event discussions etc.

The prime interests related to the services offered for these groups could be

- Event Announcements and Schedule Updates
- Calendar Sharing
- Location Based Services to identify the location of personals in time critical situations.
- Shows Details (Ramp Numbering etc.)
- Document Sharing
- Media Sharing
- Post event Comments

One of the important factors is the fact that there would be many personals in this specific group that would be member of more than one portal i.e. models, photographers. It would be cumbersome for them to manage separate identities for every portal. So the support of current identity services available in market [14] would be necessary along with other security requirements.

Some users of this group would also be reluctant to reveal their location so they should be assured of anonymity protection if they don't want to disclose their identity at particular moment along with other security features.

Another challenge would be to provide temporary access to some personals for some specific event i.e. company want to hire some specific beautician overseas for some particular event held at that country or city. Hence various user profiles should be maintained and security levels for these profiles must not be compromised.

### **2.1.2 Religious Factions**

This use case is primarily intended for religious factions living in a particular locality or county. The prime objective would be to provide them a secure mobile social group to openly discuss their beliefs, share thoughts, organize and participate in various events etc. The group would also be interested in announcing community services and checking the availability of volunteer's for that specific task. There

would be some tasks held periodically for which they would be interested to acquire some specific personals like delivering lectures, debates etc.

The services on which this group could be interested could be

- Blogs
- Daily/ weekly Updates about some holy texts etc
- Community Service Notifications
- Notifications and confirmations about gatherings
- Location based services
- Calendar sharing
- Media Sharing

The closed user group might be connected to another similar group of that particular community and user of one group must be identified by the users of the other groups in case of travel or permanent settlement to new area. Hence, providing strong authentication procedures within that group and intra group would be handy.

### **2.1.3 Business Network**

This use case primarily targets company owners, directors of investment societies, business funds, stock holders etc. This group would certainly require secure mobile social group that keep them updated about the live business activities on the go. They would like to have live updates about stock market trends, gold and currency rates, property updates etc. This group would also be interested in some sort of social portal where they can acquire these specific updates and notifications about certain commodities, discuss investment ideas with their friends and share blogs to get advice from best in specific business domain.

The type of services this group would be interested could be

- Live updates of stock market, gold, currency, property rates etc.
- Blogs
- Graphs and charts depicting previous market trends
- Reports about future analysis
- Investment port folios
- Documents Sharing

This group would certainly require all the security and portability features that have already been mentioned in fashion and religious faction use cases i.e. secure authentication, anonymity protection, authentication forwarding, managing user profiles and identity service support.

Due to the personal nature of mobile devices, there is a tendency among businessmen to store information about their investment portfolios to keep track of things on the go. Therefore, the members of this group would also be interested in content privacy both *within* and outside the group. Investors would certainly not like to reveal any clue of their portfolios based on surfing history or logs created due to their interests in some specific commodity i.e. bond, share, certificates etc.

## **2.2 Use Case Analysis**

In this section, we provide analysis of the use-cases from the business and technological perspective. In business oriented analysis, only notable social networks having large user database and impact factor are considered [9]. The originality of our use-cases and key differences from existing social networks are also discussed. The technological aspect primarily covers the tools and expertise required to implement these use cases as a final product.

### **2.2.1 Business aspect**

There is tremendous drift between all the mobile based use-cases presented above and traditional online alternatives for these types of requirements. We are only presenting some key shortcomings of traditional social networks to incorporate our requirements mentioned in the previous section. Hence there are lots of potential scenarios for simple yet secure mobile social interactions.

#### **2.2.1.1 Business analysis-fashion industry**

Up till now there is not any famous online social network that has primarily focused on the fashion industry. Therefore most of the media giants and small companies have to depend heavily on human resource departments or individual personal to manage majority of the fashion events including photo shots, media interactions etc. The public figures from fashion industry also have to compromise between two extremes of using traditional public social networks or interacting privately with their colleagues etc. Moreover celebrities have a tendency of being tentative to reveal their identity to unknown online users. So there is a big potential for secure and closed social network alternative for this specific industry. Moreover the requirements discussed in our use case can't be catered by any online social network like location tracking; privacy protection, authentication forwarding, direct mode etc that should be only focused for a specific company or media group.

#### **2.2.1.2 Business analysis-religious faction**

Although there are some online *open* social networks that are specific for some religion [10, 11] or providing some sort of association among sacred places of that

particular religion. But there are some key differences among these and our proposed mobile social group which can be summarized as follows:

- Open networks targeted to attract as many users as possible even for non-believer of that specific religion
- Primarily focused only on blogs
- No real social activity in Particular County, neither targeting any community service etc.
- No security profiles for authentication, privacy protection etc

#### **2.2.1.3 Business analysis-business network**

Just like religion, there are some notable online social networks [12, 13] targeting business community but all of them are open and primarily intended to share news and events related to business community. As already mentioned, the prime targets of references mentioned above and other networks is to attract as many users as possible and they are not concerned for providing real social activity in a closed, secure and mobile environment.

Moreover online social networks related to business are also prone for mergers with big trade companies resulting in terminating services, closing user accounts, and off course revealing the status of existing user's port folios and identity information to the new owner's. This fact alone is the biggest concern for people of business community who want to interact socially but remain updated about their business activities securely.

#### **2.2.1.4 Customized Online Social Networks**

There are some online solutions that provide facility to create custom online social networks [14]. But there are lots of draw-backs in those solutions and they lack many of the features that our proposed closed mobile social networks can offer. Only a few of large potential differences and short comings of these so called custom online social networks can be summarized as:

- Considerable fee for just customizing limited set of services
- Primarily Customer Management System (CMS) solutions, that allow minor modifications to the overall designed system and services
- Resulting solution is a typical open social network targeting as many users as possible
- Considerable overhead for setup and maintenance

### 2.2.2 *Technological aspect*

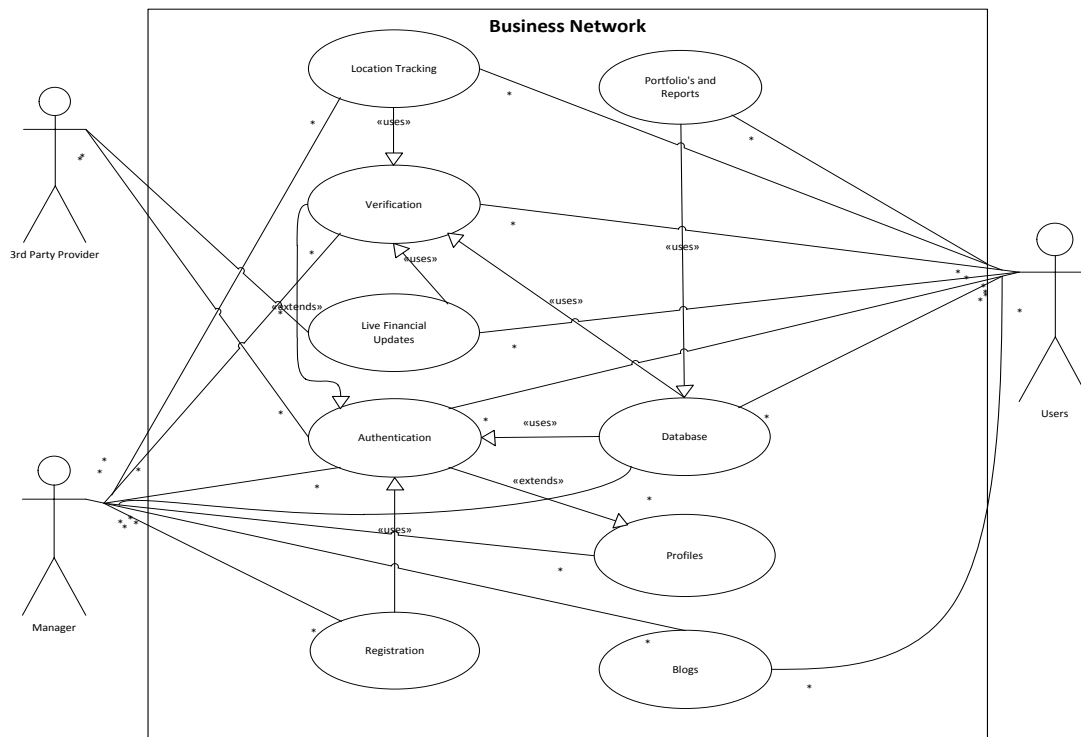
The use cases defined above poses challenge to update existing security, media sharing, content distribution standards and bringing these technologies together for realizing mobile social networks. All the use cases require a networking online portal that is accessible from mobile units. It is evident from use case diagrams that membership is restrictive as compared to traditional online social networks. Hence the portal must provide strong security guaranteeing that:

- Only invited members can join the network after strong identification and verification mechanism. If registration is triggered by some other member in offline direct mode then secure identification and authentication procedures should be implemented.
- There must be a strong authentication mechanism for user verification. Moreover in case of identity service, the overall system delay must remain under some well-defined threshold limits.
- All communication between portal, fix or mobile terminals should be protected using confidentiality and integrity protection mechanisms.
- Content storage and distribution mechanisms should be applied to prevent information leakage.
- Anonymity prevention must also be assured using updated cloaking algorithms for location based services.
- Role based authorizations support is necessary for managing access control based on users level and reducing the security maintenance overhead of moderators or super users.

The new 3-4G networks provide speed as equivalent or in some cases slightly better connectivity as compared to wired solutions. Moreover, contrary to traditional slow mobile networks and units, the new mobile units offer considerable processing capabilities to handle the online applications. Hence, all the requirements can be realized by ordinary web client by using applets and ActiveX controls. The other approach could be to develop or merge special purpose applications targeting mobile units.

Another technological aspect is to provide compatibility among current online OpenID standards with USIM architecture. The whole process should be secure, quick and must be transparent to the client in a seamless manner and should place less overhead as compared to current solutions.

The media sharing can be easily managed using Session Initiation Protocol (SIP) [15], H.264 [16] video, G.726 [17] and other ITU-T audio standards currently used by Blue Ray, YouTube etc. Similarly there are numerous solutions available for managing blogs and sharing calendar such as iCalendar [18].



Some mobile social networks would also require complete role based security model as well as support for moderators or trusted third parties (based on their specific roll) to enroll offline users to the closed group and this new user should be seamlessly supported by the other members of that specific group.

The general and simplest form of basic functional components of business network described above is depicted as an extended use case diagram in Fig. 1. The business network is supposed to be an independent system with all the functional requirements depicted as use cases. The above diagram clearly shows the challenge to cater requirements of several different closed network scenarios and to realize them through software architectures via mobile social network portal.

In summary, most of the technologies along with components already exist in form of diverse software offerings. Hence to practically comprehend secure but light weight solution, a detailed study about current security standards and ongoing research work related to requirements of use cases is required. The outcome of that study would reveal the tactical and architectural methods to bring these fractions together into final solution offerings that are related to business models.

Majority of the technological aspects discussed above could be compromised without strong key management, authentication and privacy protection support which is

backbone for the closed user interaction in secure way. In the SWIN project [1], our prime focus would be to probe and investigate the following security functions:

- Authentication and key exchange
- Secure Identity sharing in heterogeneous environments
- Anonymity Protection

## **2.3 Security Requirements**

It is evident from all the functional requirements presented at previous section in the form of use cases, that idea of closed social groups for targeted customers can only be realized by providing trustworthy and fool proof social networks in terms of security. This goal can only be achieved by identifying, listing and solving these requirements in a secure, yet efficient and user-friendly environment. The requirement set from use cases can be primarily sub-categorized among the following goals along with brief details about perspective of all the main actors involved in use cases:

### **2.3.1 *Secure Registration and Authentication***

- Only authorized client should be allowed to register in closed networks by enforcing strong authentication procedures. Strong access mechanism should be applied to eradicate fabrication and other un-authorized requests for gaining access.
- Authorized client can register new members in offline mode by strong authentication procedures in confidential manner and ensuring integrity.
- All active and passive attacks i.e. denial of service; traffic analysis etc. should be eradicated by enforcing strong authentication scheme.
- The registration and authentication process should be in compliance or extension of current GBA based [6] authentication standards.
- The whole registration process must be secure and all credentials of users should be transferred as cipher on unreliable media.
- The portal should support the current and future identity sharing standards [8, 5], in both online and offline mode.
- The authentication procedure should support proxy mechanism, where one node attached to server might act as a gateway for offline client.
- The complete data acquisition process between server and gateway should be confidential and ensure integrity of transmitted data over temporary connection.

- If a user is registered in offline mode to secure social network by another privileged user in legitimate manner, then the whole process of sharing and managing security associations in online mode should be transparent for the user and the whole procedure should be completed in seamless manner.

### **2.3.2 *Profiles and Location Based Services***

- All the users in closed social networks can't have same profiles or same set of privileges. Hence roll based security features should be supported by portal.
- There should also be an option for setting explicit security settings for scenarios where role based security should not be considered flexible by key members, and who are ready for managing overhead for this sort of management.
- The users should be guaranteed anonymity protection if they decline to register either permanently or temporarily for keeping their track through location based services.

### **2.3.3 *Access Control and Data Storage*<sup>2</sup>**

- Strong access control mechanism must be enforced to keep the user data safe both from outside and inside the network. The origin of data must also be authenticated to avoid duplication.
- The integrity of data must be verified at every instance to keep the database consistent and error free.
- Content (user identity and data) storage and distribution must be securely preserved and transferred respectively. There must be DMZ implemented at *server* level along with strong access policies to prevent any content leakage. The challenging goal would be to achieve this task without compromising on quality standards or delaying services.

### **2.3.4 *Managing real-time services***

- The mobile devices are primarily designed for providing real-time audio service (with current trends toward video calling). So all the online and offline audio/video communication must provide confidentiality and integrity support during transmission on wireless medium.
- Live streaming support should be handled by the portal in a secure yet maintaining threshold levels required for non-delayed, jitter free services.

---

<sup>2</sup> The requirements are mentioned as they relate to the identified use-cases but are not part of this particular thesis.

## **2.4 Summary**

This chapter introduced secure identification in terms of social networks in cellular domain. The chapter identifies some potential use-cases that are unique in terms of user requirements on a mobile device. The differences between existing networks entities and the proposed solution are discussed in detail to demonstrate the market potential. Also the business and technological feasibility aspects have been conferred to make these use-cases realized in the social network portal. The security requirements that are assumed to be fundamental for the topic are also identified and can be of vital importance for final prototype development.

### **3 STATE OF THE ART**

This chapter primarily provides overview about the customary concepts and standards about mobile social networks, tools and technologies already deployed along with insight about futuristic emerging trends and research activities.

As already discussed in previous chapter's that mobile social networks offer some exciting application services like location based services, instant mobile messaging, instant notifications and communication facilities in either network or direct mode (push to talk, Bluetooth, WIFI) etc. But all this excitement comes at a cost of newly evolved security threats and compromises on privacy protection. There might be limited number of people who would be comfortable to reveal their exact location of presence as a consequence of using cellular service and this aspect alone might change user perspective about mobiles being personal in near future. Moreover there is a tendency among users to carry more sensitive data on their mobiles phones as compared to typical personal computer like contacts, passwords, bank account details, updated calendars entries with key dates and personal notes. So deployment of state of the art access control mechanisms on mobile devices to keep security of content storage is a prime need. All the communications (data and voice/video) should be encrypted on wireless channel regardless of any direct, indirect or dual mode of operation.

The phenomenon of mobile social networks is relatively new and to manage all these newly emerged security threats that may prove critical in realization of real mobile social networks is a complex task and consequently popular topic of research activities around the globe.

In the following sub-sections, we provide overview of conventional online social networks history and promising applications that are main reason for popularity of traditional and mobile social networks. But our focus would be to probe notable secure identification schemes and key management standards as well as latest research trends with later as main theme of discussion.

#### **3.1 Mobile Social Networks**

The online social networks phenomenon was spotted almost a decade ago and since then it has gain revolutionary popularity. We will provide brief history of traditional online networks and emerging trends focusing on mobile social networks.

##### **3.1.1 Online Social Networks**

Social networking services were started with the intention of linking small communities and providing them interacting services that will engage them via internet [19]. The first notable social networking website was found in the year 1997 through formation of a company called Sixdegrees.com but the real boast was gained by Friendster that started its working in the year 2002 and was totally designed to

deal with the social aspect of the market. Later, MySpace gained popularity by providing some exciting features like personalizing web pages etc.

The most popular social networking site Facebook was initially launched in 2004 for college networks but later due to its easy to manage media and graphic sharing features, it gained market share outpacing its rivals with around 500 million registered users as per August 2010 statistics. Finally, another social network giant Twitter and others emerged in market basically focusing and marketing on user interaction with idea of following celebrities, friends through short messaging blogs and providing media support via third party links [19].

### **3.1.2 Social Networks in Mobile Domain**

Mobile social network is an ongoing development that is gaining ever increasing popularity among users but still needs to manage issues such as hardware limitations; compatibility and security compromises to overcome. The mobile social networks provide some exclusive new features like short messaging notification, instant messaging, and location based services etc. But the real hazard lies with trade off with the confidentiality and personal life of individual. So there is a compromise among these exciting features and one's privacy protection.

According to survey conducted in 2010 and available in [20], mobile social networks and communities continue to grow at an astounding rate. The results of survey shows that almost 72% people are accessing internet using portable devices. The results are significant as this share was only 17% in a similar survey just three years ago in United States. There are lots of other predictions that mobile units would be prime source of internet access around 2015 and beyond. Moreover cellular users are more willing to pay for content on mobile devices than their inclination on desktops for a number of reasons, including:

- Support of payment for real time services like iTunes etc.
- Nominal charges by service providers after subscribing, especially in North America.
- Ease of personalization i.e. changes of language, themes, settings etc.
- Exclusive applications and games designed for users on the go.

There are lots of social networking applications available in the market that are providing features like location awareness along with traditional social networking capabilities to attract customers. The notable social network services in terms of customer support are listed below

- GyPSii [21]
- Brightkite [22]
- Loopt [23]

The overview of these mobile supporting social networks in terms of the services, the customer trend and the supported hardware and software platforms for each of these networks is provided below.

### **3.1.2.1 GyPSii**

GyPSii combines desktop based services with extension for location based services with following main functions:

- The user can associate media, text etc with favorite places that relates to physical location using maps. The service extends to providing search for locating and finding new friends and their favorite places and to get in touch via short messaging service etc.
- The location information is automatically updated based on network ID or GPS, only if user wants to reveal its current location. The web clients using normal browser have the flexibility to reveal location by marking some place on the map.
- The user can search for nearby places that suite his interest and even filter them on the basis of known and un-known users.

GyPSii supports almost every mobile platform like Android, BlackBerry, iPhone, Java, Windows Mobile and Symbian S60. GyPSii is targeting China (already 800 million mobile subscribers) and other Asian countries by making business alliances with local companies that provide promotional coupons for restaurants etc. In February 2010, GyPSii claims to have added almost one million new customers in previous quarter [21].

### **3.1.2.2 Brightkite**

Brightkite is another social networking service that is focusing mobile users. It supports short messaging exchange like Twitter and even provides interface to Facebook, Twitter etc. Brightkite does not support automatic update of location information but user has to manually “check-in” at a location for getting visible for other users in the network. But the application can “suggest” user location based on Cell ID when the client is accessing services using mobile device.

Brightkite offers applications for Android, Nokia, BlackBerry and iPhone. Brightkite had almost 300,000 unique visitors in February 2010 but the rate drastically dropped below to 100,000 visitors in July 2010. The trend tough had reversed towards upward direction in August 2010 when the numbers of unique visitors have again reached 100,000 [25].

### **3.1.2.3 Loopt**

Loopt is another mobile based social network site that is primarily based in North America. It uses GPS for location sharing but only supports CDMA based networks resulting in very limited number of mobile devices supporting the services and depends on short messaging services for sharing location information.

Loopt had around 125,000 unique visitors in March 2010 but the figures dropped to around 110,000 in August 2010 [26].

## **3.2 Secure Identification Schemes**

Secure identification in terms of network security can be classified into various dimensions, which extend to secure registration and authentication, integrity control and privacy protection. The sub-sections below provide brief overview of available schemes and future research trends regarding traditional ad hoc networks and mobile social networks.

### **3.2.1 *Secure routing schemes in Ad hoc networks using PKI***

Ad hoc networks have gain hype in recent years mainly due to their vast potential for providing new exciting applications for civil purposes after already gaining significant popularity in military infrastructures [27]. Some approaches were presented to use public key infrastructure to enhance security of routing protocols but these approaches clearly lacked the anonymity of routing information transferred [28].

In 2007, Rongxing Lu and others [29], proposed a secure anonymous routing protocol with authenticated key exchange (SARPAKE). The scheme is based on so called Designated Vector Scheme (DVS) [30]. The DVS scheme is different from standard digital certificates as authentication using signature is only distinguishable by the intended verifier. The scheme proposed in [29], claimed to provide round trip anonymity of route along with integrated key exchange mechanism based on DVS.

### **3.2.2 *Symmetric and Layered approaches***

The detailed information about Kerberos protocol is available at [31]. Kerberos is authentication protocol based on symmetric key encryption and is widely used and implemented at intranet level with support by almost all the OS systems vendors. The protocol approach is based on pre-shared secret between server and client and can be easily understood by the diagram given below:

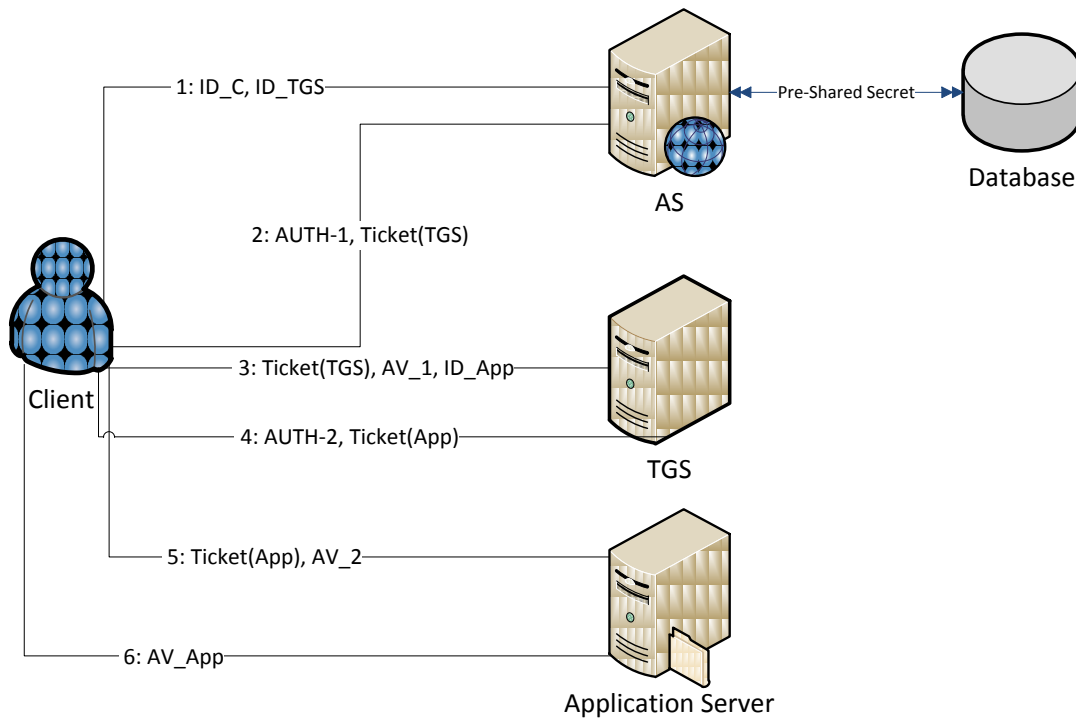


Fig. 2: Kerberos version 5 based authentication scenario [31]

The main theme of the Kerberos design was to make sure that apart from ID's of client and servers involved, everything is transmitted in cipher in the form of encrypted tickets and authenticators. The entities Authentication Server (AS) and Ticket Granting Server (TGS) shown in Fig. 2 can be implemented on same machine depending on network scalability and design. The steps shown in Fig. 2 can be summarized as:

1. During step 1, client initiates authentication request by sending its own ID and ID of TGS.
2. The AS retrieves pre-shared secret between client and TGS from database, creates session key for secure communication between client and TGS, add time stamp with lifetime and encrypts whole information with the client's secret key into single message which is referred as Authenticator (AUTH-1) in Fig. 2. Moreover the server encrypts the same information given above and the address of client for TGS using its secret key which is referred as Ticket (TGS).
3. The client provides the Ticket (TGS), along with an authentication vector (AV\_1) containing client ID, lifetime and address, encrypted by session key provided by AS in the previous step.
4. The TGS performs the same tasks as in step 2 but uses application server (App) secret key to encrypt Ticket (App) and updates time stamp and lifetime information.

5. The client performs the same procedure as in step 3, but updates time stamp and lifetime info and encrypts authentication vector with new session key obtained in step 4.
6. The application server responds with encrypted message using session key already shared, containing updated time stamp and lifetime to authenticate itself to the client.

In 2004, Asad and Chris [32] proposed a modified version of Kerberos named Kaman for dynamically incorporating the requirements of ad hoc networks. The Kaman scheme was based on multiple Kerberos servers storing hash of pre-shared client passwords and communicating with each other to update user information along with option of load sharing. Although the scheme provides secure bootstrapping and authentication support based on steps already defined above, but only under assumptions that all clients and servers have already shared the pre-shared secret in a secure way.

Due to ad-hoc nature of MANET networks, every node manages routing tables and other network and security related tasks like packet forwarding, access control etc. So some layered approaches for node level security were suggested that classify ad hoc networks in trusted and non-trusted zones and provide layered authentication approaches to provide safety from external threats along with configurations mistakes and other internal network threats [33].

### **3.2.3 Location Anonymity**

Location anonymity is major concern for exciting Location Based Services (LBSs) support available in mobile social networks and considered as main hurdle for large scale deployment of LBS as it compromises client privacy [34].

The disclosure control protocols currently in use try to solve this problem by using randomness instead of client identity and *K-anonymity factorization*. The K-factorization approach means that instead of revealing a client's exact location, the service provider would be reported cloaking area which would include at least K number of nodes. The location services are not supported if the client is at distant location and would be resumed later after re-computation of the cloaking area when the client moves closer to the other available nodes nearby. This theme inspired a lot of research publications all of which are primarily focused on minimizing cloaking area as much as possible but still don't compromise on client anonymity.

One of the researches presented in [34] is the use of entropy by considering the numbers of nodes inside cloaking area along with their anonymity probability distribution. The above paper also applies polynomial time complexity technique to set optimal cloaking area that will not compromise on user anonymity.

Another notable scheme is reporting K different footprints based on historical locations of different clients instead of computing K factor based on current locations of neighboring nodes. The main advantage of this scheme is not to update location tracking services if the client is not interested in revealing its identity as contrary to

current standards where the user must update its current location so that the algorithm can keep the cloaking area up to date [35].

### **3.3 Key Exchange Schemes**

This section is focused to provide sketch of traditional key exchange schemes used in fixed and mobile networks and their extension to incorporate the cellular nodes simultaneously. We will also probe for identity sharing mechanism like OpenID [8] that provide the facility of single sign-on (SSO) to reduce the client handling of multiple username and password pairs for different websites. There is also continuing research to provide solution for compatibility of such identity management schemes among various vendors and with USIM/ISIM standards.

#### **3.3.1 *Secure Identity Management and Sharing***

Identity sharing is an idea to provide SSO services to solve the user's problem of managing multiple login credentials for various sites. The most notable identity management providers were Windows CardSpace and VeriSign Identity Protection (also known as VIP) [36, 37]. In 2006<sup>3</sup>, a consortium comprising of various vendors was formed for providing global identity standard (OpenID) that should be transparent for end users [38, 8]. The basic aim was to develop a lightweight protocol for URL authentication using standard HTTP protocol.

##### **3.3.1.1 OpenID Authentication and Key Exchange Mechanism**

For interested readers, the detailed information about protocol architecture and the detailed specification can be found in [8]. We only focus on authentication steps and some common terminologies in this section to provide brief overview of authentication and key exchange procedures.<sup>4</sup>

- The identifier is client unique OpenID identifier in HTTP or HTTPS format.
- The user agent is client web browser that should support HTTP ver1.1.
- The Relaying Party (RP) is the application server website, where user wants to reveal identity for gaining access.
- The OpenID Provider (OP) refers to OpenID providers like Google, Microsoft etc.
- OP identifier is the identifier of the OpenID provider to the client and OP endpoint URL is a valid HTTP or HTTPS address for verification.

---

<sup>3</sup> Interested readers can find more information about identity management among vendors in [38]

<sup>4</sup> The information is extracted from [8] and paraphrased for ease of reader understanding

The steps involved in authentication and key exchange using OpenID are shown in Fig. 3. The steps marked with dashed line are optional and the complete procedure can be summarized as:

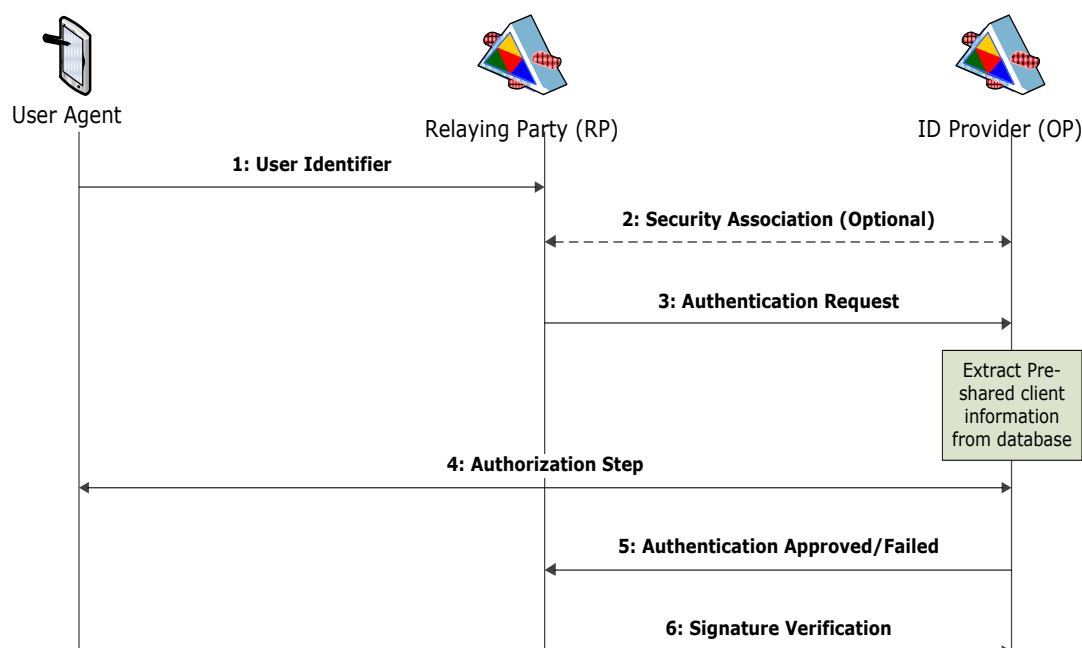


Fig. 3: OpenID Authentication flow

1. The user invokes the authentication by providing its identifier to a Relaying Party (RP) via user agent (web browser or application).
2. The RP establishes the OP endpoint URL, and (optionally) creates a security association (SA) with OP based on Diffie-Hellman Key Exchange algorithm.
3. The RP redirects the user agent with authentication request to OP.
4. The OP authorizes the client and redirects him towards the RP whether the authentication was approved or failed.
5. The RP verifies the return URL, nonce, shared key (if optional association was established in step 2) and complete authentication procedure or sends request to OP for signature verification (if SA was not established in step 2).

There is a continuing debate about security of authentication procedure provided by current OpenID standard and its poor security architecture such as non-hashed nonce etc. The vulnerabilities to man in the middle and other security attacks are discussed in [39].

Many anti-phishing techniques are presented since then in various research literatures; notable among these is HwanJin Lee and others [40]. Portable tokens (based on PKI) and authentication e-mails are suggested to prevent phishing. During signing at OP, the user should save the OP authentication number on its machine. Now every time when some RP relays any user request to OP, it should authenticate

it by verifying the certificate from client machine and also forwarding that number to the client by e-mail for verification.

### 3.3.2 Generic Authentication Architecture

The detailed information about Generic Authentication Architecture (GAA) can be found in [3]. GAA is an application layer architecture primarily developed for mobile devices and runs on top of Hypertext Transfer Protocol (HTTP). The specification is used to provide mutual authentication support between User Equipment (UE) and Network Application Server (NAF) that may support heterogeneous applications. The main advantage of this scheme is to reduce the client effort for managing multiple authentication profiles for different types of mobile applications along with much improved levels of security.

The GAA supports two different types of authentication mechanisms where the first mechanism rely on symmetric encryption scheme using pre-shared secrets and the later uses public key cryptography with (public, private) key pairs and digital certificates. GAA relies on 3GPP AKA mechanism to share common secret between clients and application servers [3].

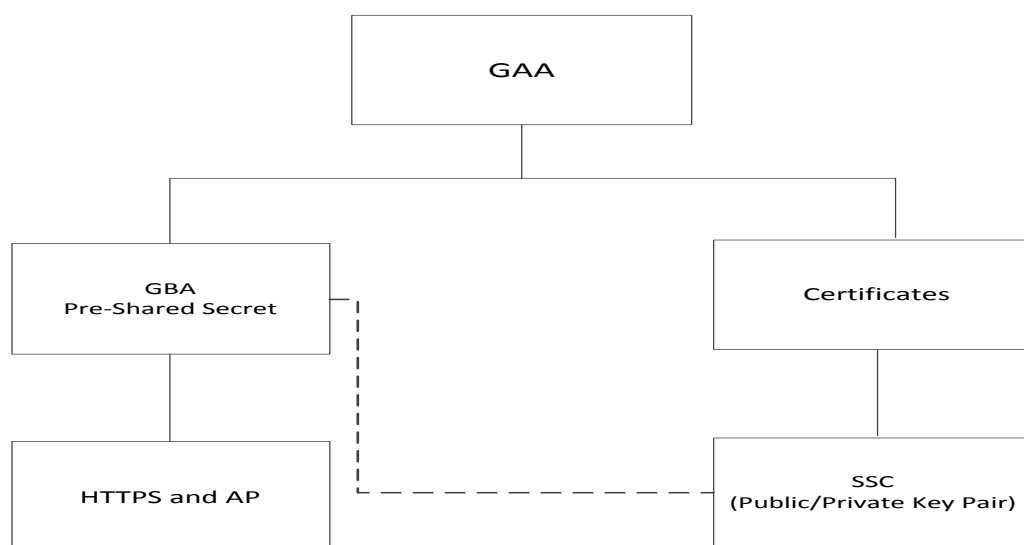


Fig. 4: GAA Architecture

The general usage of GAA shown in Fig. 4 can be summarized as:

- The pre-shared secret is used for mutual authentication between user equipment (UE) and MNO. All future session keys can be fetched from the operator based on this secret. This procedure is also referred as Generic Bootstrapping Architecture (GBA) [6].
- “In the second case, GAA is used to authenticate a certificate enrolment request by the client. Initially, the bootstrapping procedure is carried out as in the previous case followed by the client request for certificates from the

operator's PKI infrastructure, where the authentication is done by the session keys obtained by accomplishing the bootstrapping procedure. These certificates and the corresponding key pairs can then be used to produce digital signatures for e-commerce applications or to authenticate to a server instead of using the session keys" [2, 3].

- The support for Subscriber Certificate (SSC) can be performed by either pre-loading the certificate in Universal Integrated Circuit Card (UICC) or dynamically by obtaining digital certificate.
- Finally the Authentication Proxy (AP) is used for communication with several application servers (AS) in transparent manner and thus reduces the computational overhead of client device due to less Transport Layer Security (TLS) sessions.

### 3.3.3 Generic Bootstrapping Architecture (GBA)

The detailed information about generic bootstrapping architecture can be found in [6]. GBA is referred as the 3<sup>rd</sup> Generation Partnership Project (3GPP) standard for providing secure bootstrapping functionality between user equipment, mobile network operators and various application servers.

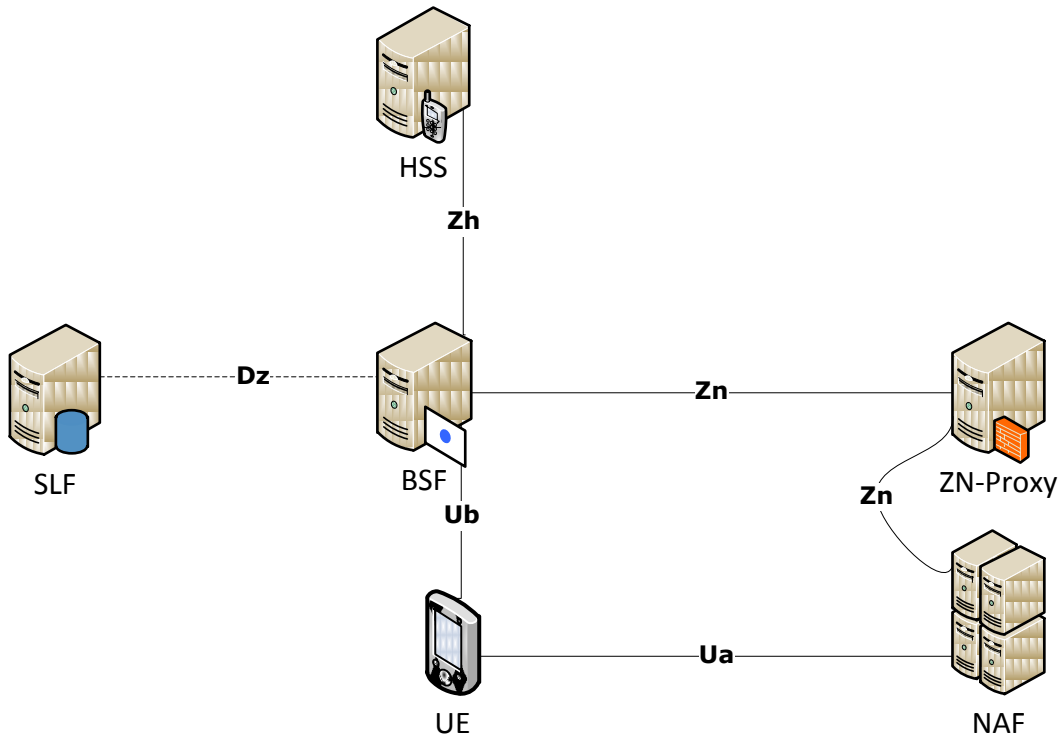


Fig. 5: GBA network model with application server outside internal network [6]

The old standard that uses mobile equipment to store authentication details was referred as GBA\_ME, with the new GBA\_U standard storing these details on UICC based SIM cards for added security protection and scalability. Although the GBA do not provide single sign-on service (SSO) like OpenID, the basic idea was to securely authenticate mobile users for various application servers by using pre-shared security

information among the operators and end-users stored in SIM cards. There are lots of changes among the old GBA\_ME, and new USIM based GBA\_U standard that is updated on new UICC compliant SIM cards but after assuring backward compatibility support.

The GBA network model is shown in Fig. 5. The UE performs authentication with bootstrapping server function (BSF) maintained by MNO. The UE and BSF mutually authenticate each other using HTTP digest AKA protocol [41] using Ub interface. The user communicates with the network application server (NAF) using Ua interface. The NAF can be internal application service maintained by the MNO or any external application using heterogeneous protocol. In later case, the NAF must communicate with the BSF using Zn-Proxy over the Zn interface. The Zn-proxy is not required if both BSF and NAF are on the same mutually trusted MNO network. The BSF communicates with Home Subscriber System (HSS) which stores the pre-shared secret (IMSI etc.) over the Zh interface using Diameter Base Protocol [24]. If MNO maintains multiple HSS then BSF must communicate with Subscriber Location Function (SLF) over Dz interface to determine the HSS to use. The usage of SLF is optional and depends on network model of MNO [6, 2].

### 3.3.3.1 Bootstrapping Procedure

The UE must perform a bootstrapping procedure with BSF whenever it wants to access some application from AS whether internally or using Zn-proxy. Once the bootstrapping is accomplished, the UE should be required to repeat the same procedure if the lifetime of session keys have expired or if some AS requires bootstrapping re-negotiation.

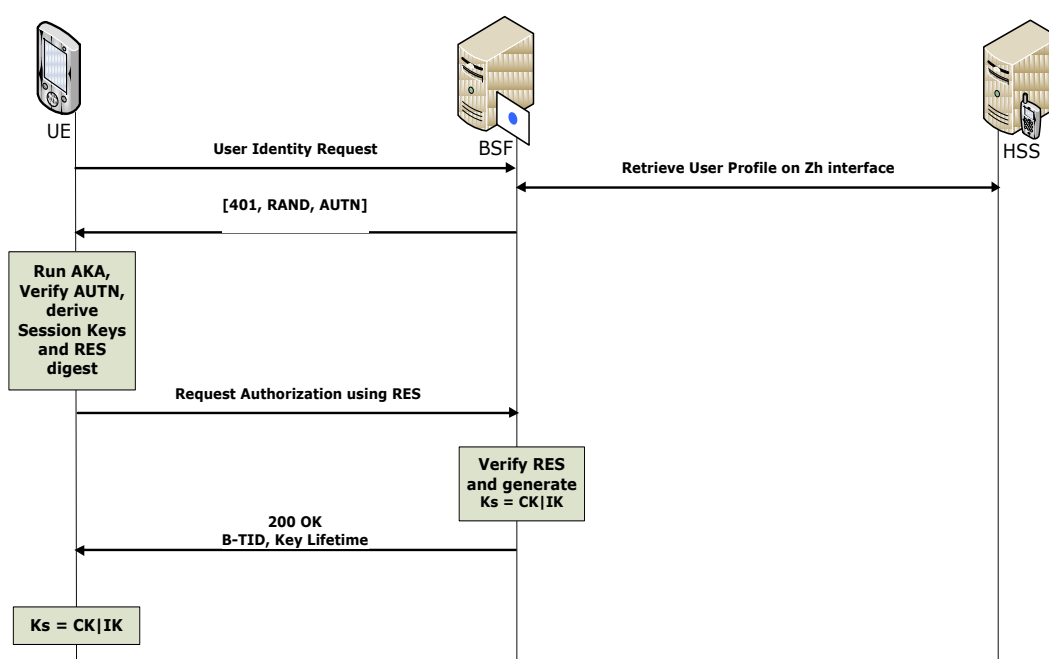


Fig. 6: Bootstrapping procedure [6]

The UE initiates the authentication request in Fig. 6 and BSF retrieves the user profile and GBA user security settings (GUSS) information from HSS, computes cryptographic vectors and forwards that encrypted challenge to the UE based on TLS tunnel along with typical HTTP 401 un-authorized response. The user computes its response and sends back to BSF which verifies it and calculates bootstrapping transaction identifier (B-TID) and lifetime of Ks based on cipher key (CK) and integrity key (IK). User calculates Ks based on B-TID on its UE and stores it in UICC in case of GBA\_U or mobile equipment if GBA\_ME is used to complete bootstrapping procedure [6].

### 3.3.4 Support for subscriber certificates (SSC)

The detailed information about support for subscriber certificates within GAA framework can be found in [42]. The SSC mechanism was developed to support global standardization of authorization and charging infrastructure for mobile commerce, building global public key infrastructure (PKI) along with local architectural support for digital signatures. The important notion about local architecture is that every MNO can implement its own architecture for digital signatures independently [42].

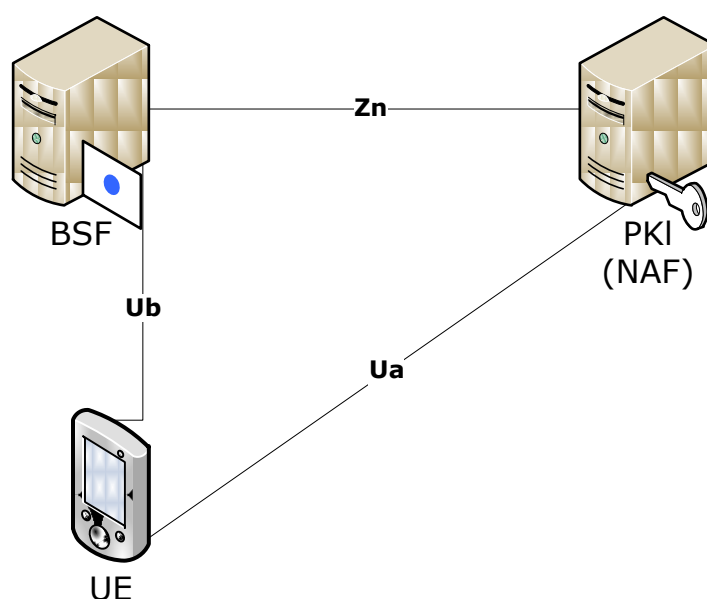


Fig. 7: Reference model for issuance of certificates [42]

The PKI portal tasks in above figure can be classified in two dimensions. Firstly it should be able to issue a certificate for client requested application using B-TID trust already developed during GBA process using reference point Ub. However, later it can also act only as a registration authority (RA) for some existing PKI infrastructure and operator certificate (CA) would be stored in PKI infrastructure [42].

### 3.3.4.1 Certificate issuing architecture

The reference point Ua in Fig. 7 is used for verifying client key pair and issuance of MNO certificate to the UE. The architecture must also support wireless integrity module (WIM) [43] support which can store private key information on UICC in GBA\_U [42].

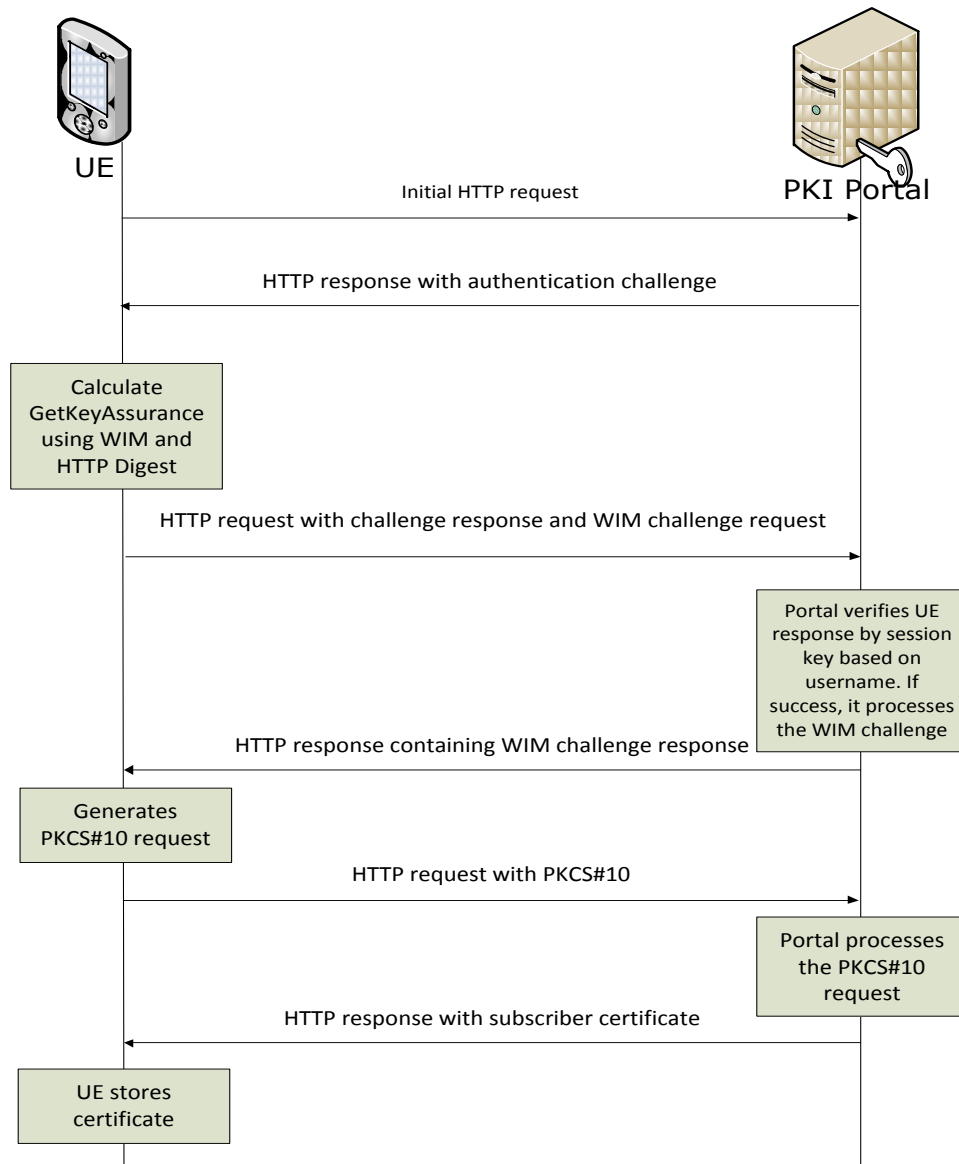


Fig. 8: Message flow for issuing certificate [42]

The UE in above figure sends empty HTTP request for certificate to NAF over Ua reference point. The PKI sends Authenticate header with typical HTTP 401 unauthorized response. The UE now uses its B-TID obtained during GBA process from BSF along with optional WIM challenge to the PKI. The PKI must interact with BSF to fetch NAF specific session key Ks\_NAF to verify user response. The PKI uses GUSS for optional WIM challenge response. The client send PKCS#10 [42] based digested request which is followed by certificate integrity protected using

Ks\_NAF. The client stores the obtained certificate either on ME or UICC based on internal management system [37].

### 3.3.5 SPKI and SDSI

Simple Public-Key Infrastructure/Simple Distributed Security Infrastructure was primarily designed as an alternative to the X.509 standard in early 2000 to provide access control and flexibility to secure distributed communication in non-trustable environment [45].

The main advantage of this scheme was support for group management using bottom up approach without any global hierarchy and trusted root that will lead to delegate authorizations. The main idea was to deal every public/private key pair as a certificate and build a guard model that is basically providing access controls to a particular object or resource by assigning, revoking and updating the giving set of authorizations [46].

### 3.3.6 Device Pairing

Device pairing over insecure wireless channel without the aid of any external link or mutually trusted 3<sup>rd</sup> party relies heavily on strong key management and authentication procedures. The notable solutions for such problems are defined in [47, 48]. These solutions can provide basic foundation for secure authentication of two devices in offline mode and can be easily modified for exchange of certificates and other services. The solutions differ slightly based on device capabilities available with user or required input by the device operator.

The solutions can be categorized as: “using data output of one device as input of 2<sup>nd</sup> device, comparing output of both devices and entering same data into both devices” [47].

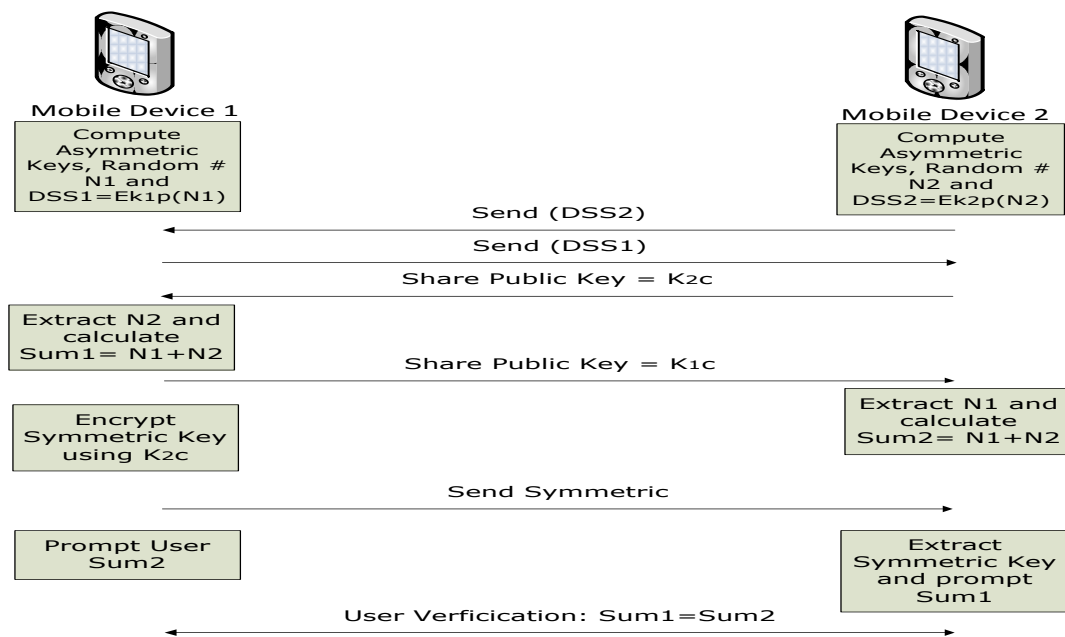


Fig. 9: Device pairing using user verification scheme [48]

The work done in [48] is based on comparing output of both devices and can be easily understood by the Fig. 9. Both parties calculate asymmetric key pair of public ( $K_c$ ) and private ( $K_p$ ) keys along with random numbers  $N_1$  and  $N_2$ . The random numbers are signed using private key and shared among devices. In next step public keys are shared to read signed messages of previous step and both parties calculate sum of corresponding random numbers. The symmetric encryption key used for confidentiality for further session is shared in next step and decrypted using already available public key of other user. Finally the user manually verifies the Sum on both devices to complete the authentication step [48].

### 3.3.7 *Manual Authentication Using MAC (MANA III)*

MANA is set of authentication protocols that are primarily used for mutual authentication among mobile nodes without the need of any 3<sup>rd</sup> party mediation or where the communication with 3<sup>rd</sup> party itself can't be trusted. The protocol family has different variants based on user input and device characteristics used by user during authentication process. In one scheme, devices should be equipped for taking input from user and typing some string on both or one mobile units involved. Another scheme is to verify the output of both devices by visual means without any need to input some shared string and thus only display on UE is required. The detailed information about these protocols can be found in [47].

The MANA III variant which is based on Message Authentication Code (MAC) scheme and requires users to input same string on both devices is shown in Fig. 10. Suppose two users A and B want to communicate using mobile devices 1 and 2 respectively. Subsequently, following are the steps mentioned in [47] for performing secure pairing.

1. Both parties must agree on shared data string  $D$  over wireless channel.
2. Both users enter a short random string  $R$  of length around 16-20 bits in their devices.
3. The user A on Device 1 generates a random MAC key  $K_1$  and compute hash of  $R$ ,  $D$  and identifier of A, say  $MAC_1$ . The user A sends  $MAC_1$  to user B.
4. The user B on Device 2 generates a random MAC key  $K_2$  and compute hash of  $R$ ,  $D$  and identifier of B, say  $MAC_2$ . The user B sends  $MAC_2$  to user A.
5. After receiving  $MAC_2$  from B, A sends the  $K_1$  to B.
6. The user B computes  $MAC_1$  from  $K_1$  received in previous step and verifies it by comparing with  $MAC_1$  received from A. If the value of  $MAC_1$  is same then user B selects OK message and sends  $K_2$  to A.
7. The user A computes  $MAC_2$  from  $K_2$  received in previous step and verifies it by comparing with  $MAC_2$  received from B. If the value of  $MAC_2$  is same then user B selects OK message to complete successful pairing.

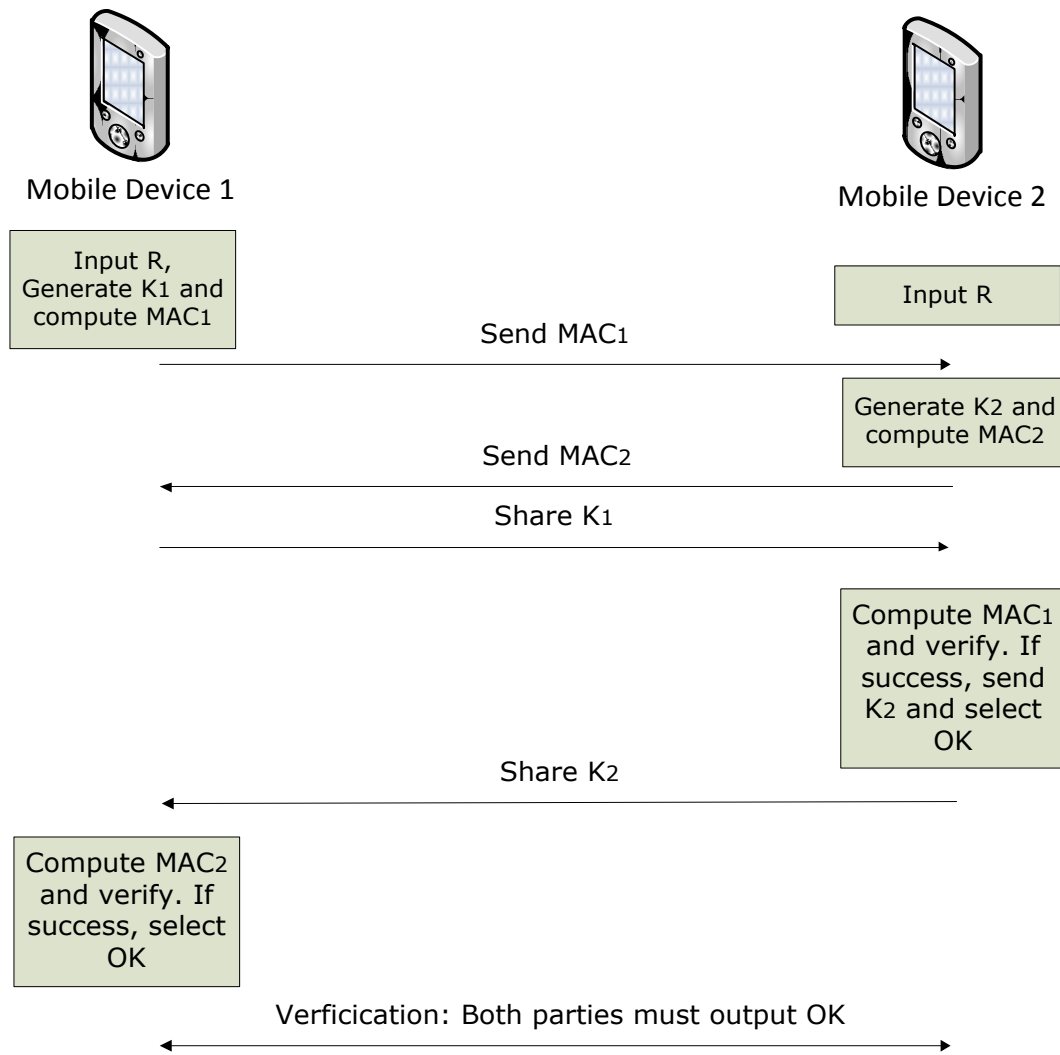


Fig. 10: Manual authentication using MAC [47]

### 3.4 Transport Layer Security (TLS)

The detailed information about Transport Layer Security (TLS) is available in [49]. TLS is successor of Secure Socket Layer protocol (SSL) which was originally developed in 1995 by Netscape Corporation to secure communication over internet using their web browser. The protocol was later standardized in 1999 by internet engineering task force and its basic architecture is almost the same as SSL but with some functional changes to improve security i.e. additional alert messages, more resistance to DOS attacks etc.

Application (HTTP)		
TLS Handshake Protocol	TLS Alert Protocol	TLS CCS
TLS Record Protocol		
TCP		
IP		

Fig. 11: TLS Protocol Stack [49]

TLS is based on client/server architecture and runs on top of TCP protocol (although new variants support UDP) at transport layer as shown in Fig. 11. The protocol uses asymmetric encryption for authentication and key exchange (RSA and Diffie-Hellman etc), symmetric encryption (RC4, DES, 3DES, IDEA etc) for confidentiality of communication and hashing algorithms (MD5 and SHA-1) for providing integrity. TLS is the primarily superset of four different protocols to secure communication among client/server using a single or multiple simultaneous connections. We provide overview of these protocols below:

### **3.4.1 *TLS Handshake Protocol***

The handshake protocol is used for key exchange, authentication and establishment of logical connection between the communication parties. All the cryptographic negotiations, authentication vectors for session setup and keys for further communication are derived during handshake process. The handshake protocol is illustrated in Fig: 12 and uses eight compulsory and five optional messages. The optional messages are shown as dashed lines and the total procedure can be summarized as:

1. During step 1, the client initiates a session by sending Hello message. The client hello message include following information.
  - Version Info
  - Session ID
  - 32 byte random number
  - Cryptographic details (browser support for encryption, hashing, compression etc)
2. The server gives its response by sending server Hello message, by selecting the cryptographic parameters included in client Hello along with its version support and random number. The server may optionally provide its certificate and may demand for client certificate.
3. Notification to the client along with server public key.
4. The client may provide certificate if server has requested, compute 48 byte master secret from random numbers of server and client and pre-master secret. The clients also encrypts pre-master secret from server public key received previous step and send it to the server.
5. The client generates session keys from master secret and sends CCS message to notify server that the further communication would be encrypted using the cryptographic parameters already negotiated. CCS is a separate entity and not part of handshake protocol but mandatory during handshake procedure.
6. The client notification to server that it's computational processing has finished.

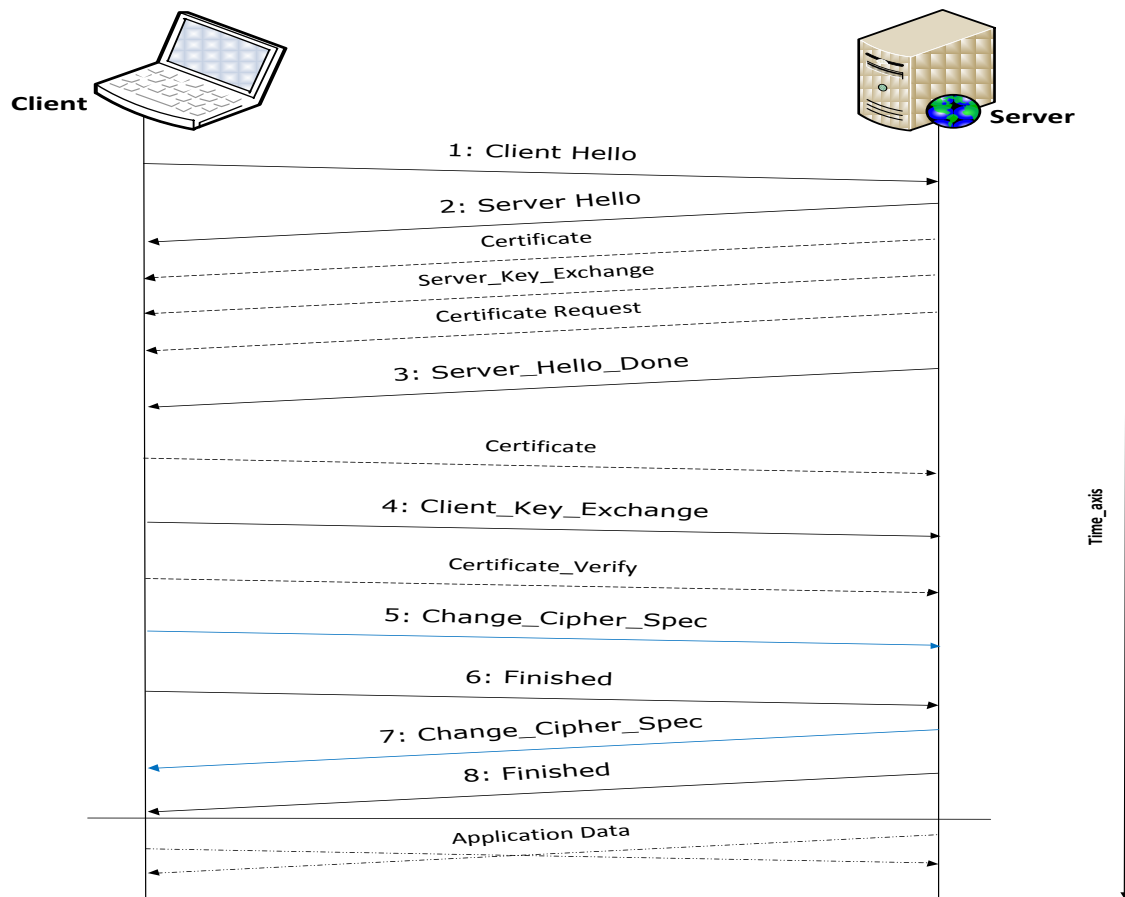


Fig: 12: TLS Handshake Protocol [49]

7. The server must compute the master secret and session keys. The server must ensure that it must use the same cryptographic parameters (pre-master secret) sent by the client during step 4.
8. The server sends finished message. Note that in SSLv3 the client was able to start sending application data without waiting for server finished message but this procedure has been changed in TLS. The client cannot start encrypting application data unless it receives server's finished message.

### 3.4.2 TLS Change Cipher Specs (CCS)

This is one byte value that is shared during handshake protocol to notify the other party about the current cryptographic parameters used and for verification of the active state.

### 3.4.3 TLS Alert Protocol

This protocol is used for keeping the other party up-to-date with the state of connection and these messages are encrypted using active state parameters negotiated during handshake. The alerts are of type “warning” and “fatal”. If a alert is received from either of the communication parties having type “fatal”, the

communication among parties is immediately terminated i.e. decompression\_failure, certificate\_revoked etc.

#### **3.4.4 *TLS Record Protocol***

The record protocol is responsible for fragmentation, encryption, hashing and optional compression of data during sending and performs the vice versa operations at receiving side.

### **3.5 Summary**

This chapter provides overview of the customary concepts and standards about mobile social networks and the available tools and technologies. The chapter has provided insight towards the existing social networks within the mobile domain and services offered by them. It has highlighted the customer trends towards these networks which can be helpful for determining the future predictions. Moreover, the chapter has also provided necessary details to understand main tools and technologies already deployed, along with the insight about futuristic emerging trends and research directions. The chapter clearly illustrates about short comings of existing solutions and protocols to cater the requirements of secure and interoperable mobile social networks and motivates for enhanced research activities.

## 4 SECURE IDENTIFICATION DESIGN

This chapter provides the details about solution based on fulfilling the requirements discussed in the previous chapters. This specification provides architecture for the secure identification, to support Mobile Social Network Portal (MSNP) in both offline and online mode.

The solution comprises of typical online identification, authentication using TLS along with offline authentication and key exchange mechanisms in compliance with Generic Authentication Architecture (GAA) specification. We have chosen the certificate sharing mechanism for performing secure identification and authentication of a user due to number of technical reasons described later in this chapter. The Network Elements (NE), interfaces, cryptographic parameters and detailed procedures for authentication and key-exchange are also presented.

### 4.1 Architecture Overview

Fig. 13 shows the network model for extending GAA infrastructure for bootstrapping and certification and its extension to support MSNP.

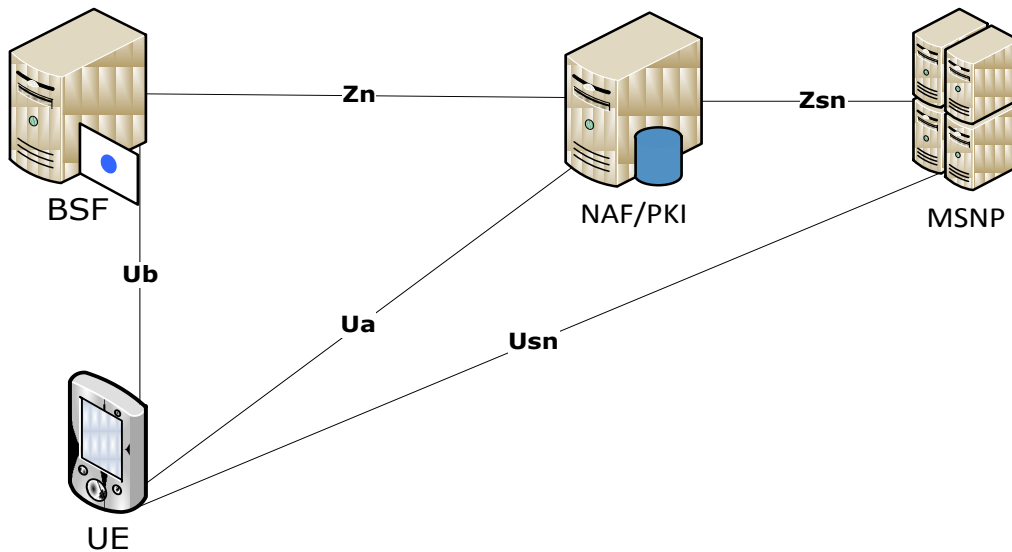


Fig. 13: Simple model for mobile social network portal

The solution is based on public/private key pairs and corresponding certificate signed by the PKI portal managed by the Mobile Network Operator (MNO). The solution can be distributed among following networking elements:

- The security profile needed for bootstrapping is being named as User Security Settings (USS) and is managed by the PKI portal over Zn interface or via Zn-proxy in case of foreign network.
- The MSNP would extend these USS for issuing, delivering and revocation of certificates. This particular set of data gathered from the user including

additional information related to certificates structure would be termed as MSNP based User Security Settings (MUSS) in rest of the document. The MUSS is needed to specify the role of specific user within various social groups.

- The bootstrapping procedure and agreement on session keys to be utilized by the MSNP would be managed using standard GBA bootstrapping procedure defined in 3GPP TS 33.220 [6] over Ub interface. The PKI portal will manage certificates as mentioned in 3GPP TS 33.221 [42] specification based on USS and an extension for secure mapping using local profile information obtained from MSNP.

#### 4.1.1 Certificate Structure

The certificates *should* be issued using X.509 version3 extended certificate format as mentioned in RFC 3280 [49]. The X.509 version3 allows flexibility for having additional attributes apart from compulsory standard attributes in certificate extension. One example can be the “explicitText” field attribute in standard extensions which allows organizations to insert 200 characters string directly into the certificate to manage the additional set of identities required. This field should be used to include the group identification information of specific closed group in MSNP.

#### 4.1.2 Database Model

The database model for authentication module of MSNP is shown below. The model does not include the format of managing certificate store at PKI portal, trust hierarchy towards operator root certificate etc. The model presented below only provides facility for secure mapping of MSNP based User Security Settings (MUSS) to support issuance/updating the social certificates issued to users interacting within various closed social groups. The certificate issuing and management procedure will follow the 3GPP TS 33.221 [42] specification with an addition to secure mapping over Zsn interface and issuance of social certificates to the MSNP user.

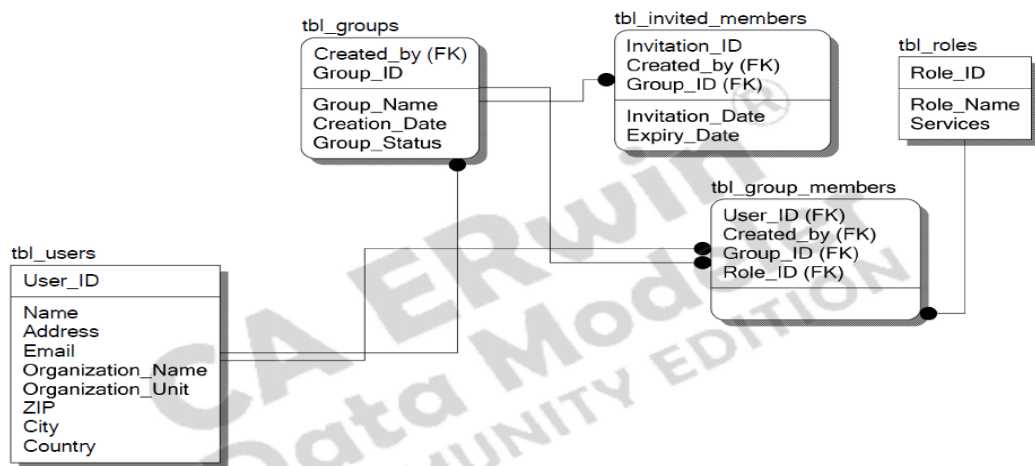


Fig 14: Database model for MSNP secure identification module

#### **4.1.2.1      tbl\_users:**

The table will include unique identification of the registered user along with other attributes. The proposed User\_ID should be MSISDN of that user.

#### **4.1.2.2      tbl\_groups**

The table will store records of all mobile social network groups. The table will maintain User\_ID as foreign key for group moderator, date of creation and group status to check whether the group is kept in active state by the moderator.

Note: There can be more than one moderator of the same social group. The 'tbl\_group\_members' table will identify those roles. The created by attribute of this table is for unique identification of group creator who can deactivate/activate the particular group later.

#### **4.1.2.3      tbl\_roles**

The table will store the defined roles by the MSNP associated with unique 'Role\_ID' like moderator, member, temporary member, pending etc.

#### **4.1.2.4      tbl\_group\_members**

The table consists of foreign keys to uniquely identify the user belonging to specific group and their corresponding roles. The table can be implemented as database view instead of physical table depending upon implementation.

#### **4.1.2.5      tbl\_invited\_members**

This table will store status of all the online invitations by various group moderators. The table will uniquely identify the invitation and their expiry date set by moderators.

## **4.2      Networking Elements and Requirements**

The required functionality for the networking elements shown in Fig. 13 can be summarized as:

### **4.2.1      *User Equipment***

The user equipment must support all the requirements mentioned in 3GPP TS 33.220, 33.221 [6, 42] with following additional functionality:

- The UE must install plug-in for browser for managing additional certificate enrolment and signing procedures to communicate securely over Usn interface with the MSNP.
- The plug-in and client application should be able to interact with NAF/PKI using HTTPS protocol with TLS extensions support as mentioned in RFC 4366 [50].

- The UE will maintain certificate store to store its certificates along with the public/private key pair. The access control mechanism to ensure device security is out of scope of this thesis.

Note: To support offline communication with other registered users and use offline features of MSNP, the user should be recommended to install client version of the application.

#### **4.2.2 Bootstrapping server function (BSF)**

The BSF must support all the requirements mentioned in 3GPP TS 33.220, 33.221 [6, 42] with an addition to the support MUSS which are needed to issue, update or revoke social certificates.

#### **4.2.3 PKI**

The PKI portal must support all requirements mentioned in 3GPP TS 33.221 [42] and NAF requirements specified in 3GPP TS 33.220 [6] with following additions:

- The PKI must support HTTPS with TLS server extensions as mentioned in RFC 4366 to securely communicate with UE over Ua interface.
- The PKI portal must complete the GBA bootstrapping procedure using specific User Security Settings (USS) obtained over Zn interface from BSF to authenticate the UE and update MSNP over Zsn interface.
- The PKI portal will provide mapping to the MSNP requests for verification of client after generation of key pair using GBA upon successful completion of authentication procedure over the Zn interface. The PKI portal will create, update and revoke certificates for the user.
- There would be already a PKI portal managed by the MNO for certificate issuance, revocation for other applications. The PKI portal supporting MSNP will only provide the GBA based User Security Settings (USS) along with certificate hierarchy and revocation lists.

#### **4.2.4 MSNP**

The MSNP would manage:

- Issuance and updating the social certificates to the users. The MSNP database would manage group creation, login facility to the online users etc as shown in Fig 14.
- The profiles/roles of all registered, invited users. These profiles would be linked with different social network identities, as moderator of one social network might be the ordinary user of another social network.

- The mapping that will authorize users inside one social network to use various services is based on user roles within specific social group.

#### **4.2.5 Reference point Zsn**

During authentication and key-exchange phase the reference point Zsn is used for:

- The MSNP would relay the user's registration/authentication requests to the PKI portal over Zsn.
- The PKI portal will provide registration confirmation/failure response.
- The Zsn would be used for searching PKI repository for registered users of some other application managed by MNO or to MSNP for mapping of social certificates based on MUSS to enforce authorization.
- The users already registered to MSNP and holder of CA signing and social certificates should be authenticated using mapping between PKI and MSNP based user security settings, without invoking the GBA procedure over the Zn interface with BSF.

#### **4.2.6 Reference point Ub andUa**

The reference points Ua and Ub should support all the requirements mentioned in 3GPP TS 33.220 [6] to mutually authenticate UE and BSF using HTTP Digest AKA protocol, certificate request and response, certification of public keys, XML encryption etc.

#### **4.2.7 Reference point Usn**

The Usn interface should support all requirements of Ua interface with addition to:

- Support XML encryption and integrity standards [51].
- Usn may support TLS extensions as described in RFC 4366. This will facilitate virtual hosts over single physical address to provide transparent communication for UE towards PKI/NAF and MSNP.
- The identification, verification and registration of the user presenting invitation XML structure "InvStruct\_N" to the MSNP, obtained from moderator after offline invitation.

### **4.3 Key Exchange Scheme**

The solution comprises of providing secure registration, certificate enrollment and mutual authentication in both online and offline modes. There are various possible

set of scenarios in each mode and every scenario as well as certificate enrollment, sharing and authentication procedure can be elaborated as:

#### **4.3.1 User Certificate Enrollment**

Each MSNP will issue three certificates for identification, verification and maintaining status profile within each social group. The basic requirements and the type of certificates issued to cater these demands within the solution can be summarized as:

- 1) Every MSNP user will be issued one identity certificate for secure identification. Let us call this AuthCert\_A, AuthCert\_B etc. (for user A, B...).
- 2) The user should be able to verify different service requests etc. To ensure this, every user will be issued a signing certificate, SignCert\_A, SignCert\_B etc. (for user A, B...).
- 3) The MSNP registered user and holder of identity and signing certificates can be a part of more than one social network. Moreover the user might have different roles within different networks and these roles may change over time. So each user also has an additional certificate for verification of his/her membership and specific role in different groups. This certificate includes all groups that the particular user is a member of and the status of the group. This certificate will be referred as SocialCert\_A, SocialCert\_B etc. (for user A, B...). The SocialCert must also contain pointers (One-way hash over the complete certificate or just the public key) to the AuthCert and SignCert.

Note: The certificates can expire and revoked in a number of scenarios mentioned in 3GPP TS 33.221 [42]. The joining of new group or any change in user status in MSNP database will result in updating of his/her social certificate. This includes a repeated GBA bootstrap procedure and the issuing of a new “SocialCert” to that particular user.

#### **4.3.2 New registration and creation of new social group**

When the UE communicates with the MSNP via browser, it is instructed to download and install the MSNP plug-in for browser or MSNP client application to the UE.

Note 1: The plug-in support should provide platform independence as the client might be using other mobile operating system than supported by the MSNP client application. In case, if the UE selects to install MSNP client application, then the client might be opted to install additional plug-in available for the browsers providing him option to communicate with MSNP without using client application.

Note 2: The interoperability support for OpenID infrastructure as defined in 33.980 can also be supported later.

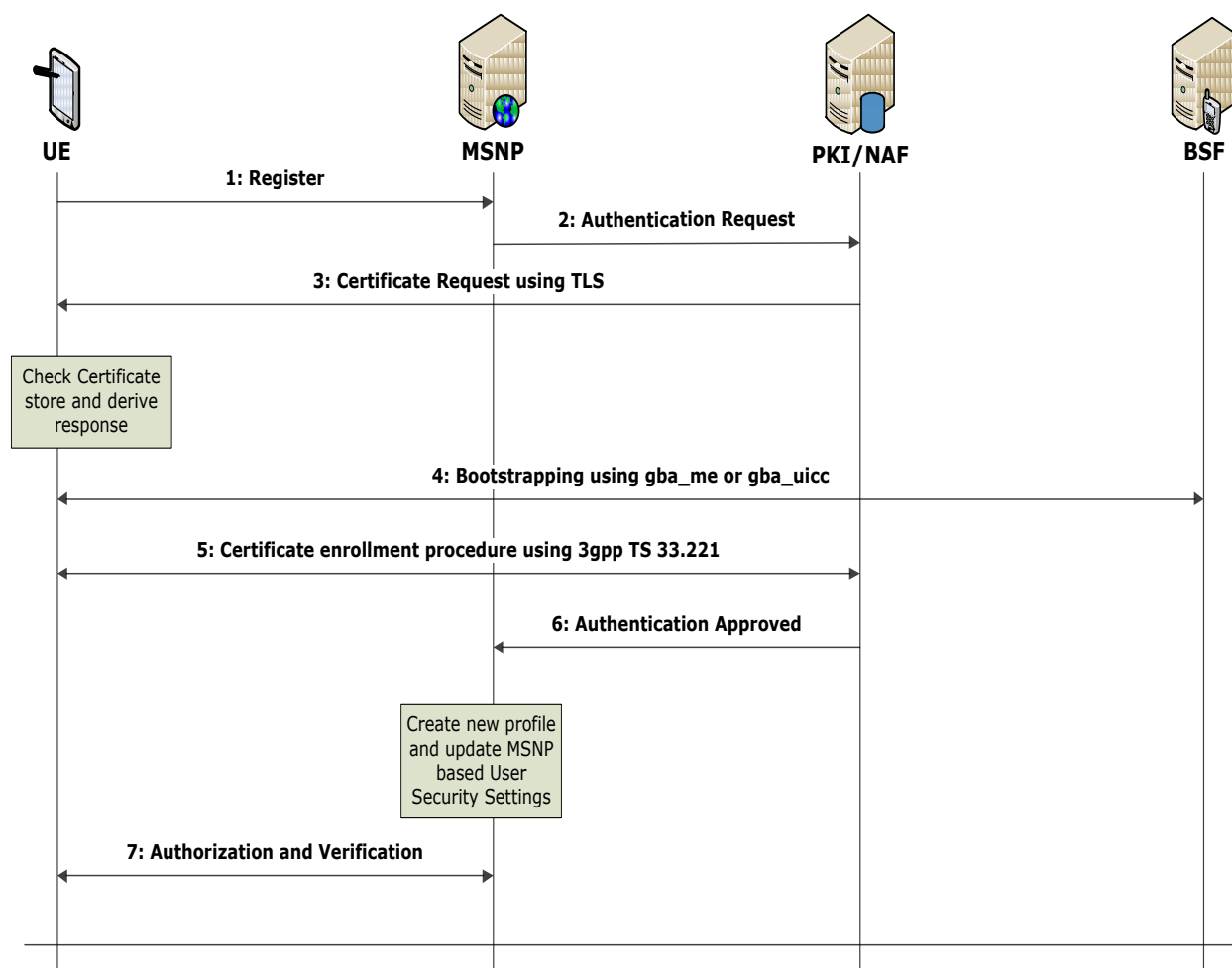


Fig. 15: New user registration flow

1. The UE will start TLS secure session with client using already installed plug-in or client application. MSISDN should be used as client id for initiation of secure identification procedure.
2. The MSNP will verify the identity of the UE to establish that the UE is new user or an existing MSNP user. In later cases, it will forward UE request for registration or communication along with MSISDN to the local PKI/NAF for verification of authenticity. The PKI portal will send certificate request message to UE.
3. The UE will check the supported certificate list mentioned in certificate request message and reply with empty response (UE can reply with operator AuthCert if it already holds such certificate in its certificate store). The PKI/NAF will initiate bootstrapping procedure and request UE to start GBA based authentication procedure. The UE and BSF will mutually authenticate

each other over Ub interface and derive session keys using AKA protocol as mentioned in 3GPP TS 33.220 [6].

4. The UE will respond to PKI/NAF with B-TID obtained via GBA process in previous step. The BSF will validate this B-TID with BSF over Zn interface (via Zn proxy in case of foreign network) as mentioned in 3GPP TS 33.220 [6].
5. If the client is authenticated then the client will be issued new authentication and signing certificates signed by PKI portal according to the 3GPP TS 33.221 [37] specification using X.509 certificate structure.
6. The PKI/NAF will update the MSNP application over Zsn interface and user registration process will be completed. Furthermore, user would be able to create new social group with active status. New social network with unique name/ID is created and MUSS is updated with MSISDN of that UE as moderator of that particular social network group.
7. The MSNP will securely interact with UE to allow user to use social network group and assign the particular MSISDN as moderator of that group as role status. The MUSS for this particular user is updated to the PKI over Zsn interface, which will create new social certificate and deliver to the client over Ua interface.

#### **4.3.3    *Secure authentication of registered users***

The registered users of MSNP already contain unique “User\_ID” for MSNP and would be holder of authentication and signing certificates. The users that are member of any social group would have an additional social certificate stored in their ME or UICC issued by PKI using the procedure described in the previous section. The users should be able to

- Perform mutual authentication with MSNP using AuthCert issued by the PKI using TLS handshake.
- Access services of those social groups that he/she is already member off by using the login information as shown in Fig 14 or by using SocialCert after establishment of secure connection with MSNP.

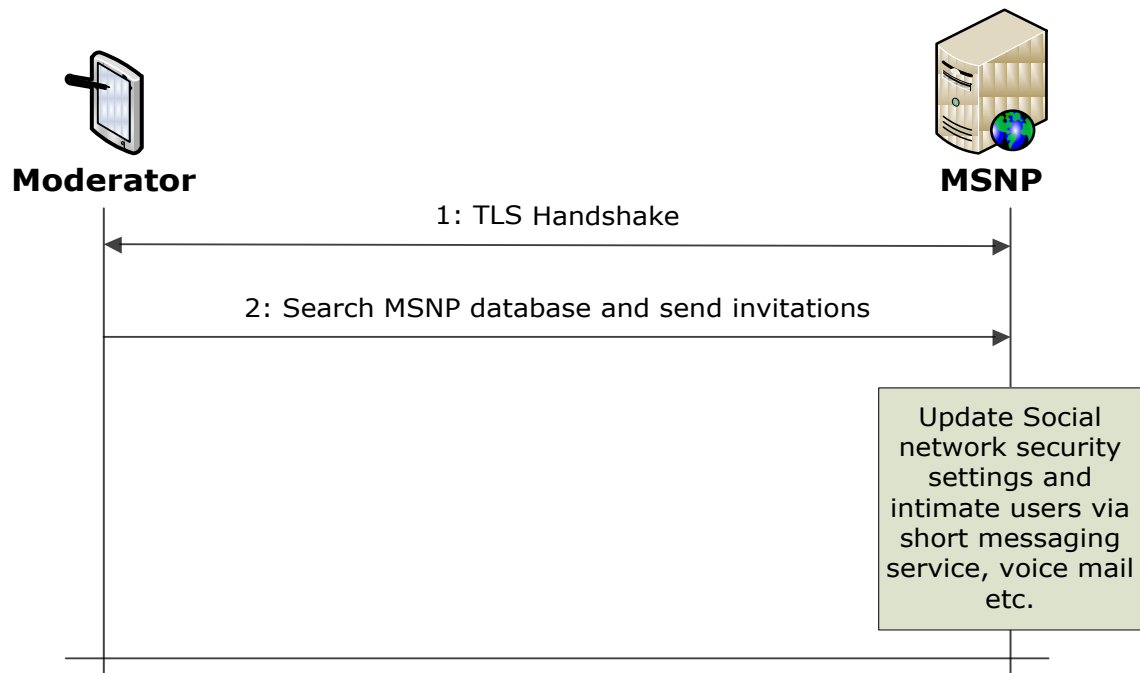


Fig. 16: Online invitation flow initiated by moderator

#### 4.3.4 Online invitation to new members

The procedure is shown in Fig. 16 and can be summarized as:

- The moderator should securely perform mutual authentication with MSNP using the authentication certificate issued by PKI over HTTPS connection.
- The moderator should have group access using database login or via social certificate of that particular group.
- The moderator of the group can either explicitly invite new members using MSISDN or by searching the interface provided by the MSNP.
- The entry of invited user would be updated in the database.
- The same request of any registered but un-authorized user (not moderator of that specific social group) would be marked as invalid by the MSNP after validating “Role\_ID” with “Group\_ID” using MUSS as mentioned in the Fig 14.
- The MSNP will update its “tbl\_invited\_members” table as shown in Fig 14 for that specific group and insert the ID’s of the invited members.
- The invitation request would be forwarded to the invited MSISDN via sms, voice mail etc.

- Users might show their intention to join some specific social network. Instead of starting complete authentication procedure, the notification will be passed on to the moderator to allow them to join group.

Note: The notification to the moderator about the interested users is subject to security settings of that particular group adjusted by the moderator. By-default this feature would be disabled to eliminate the un-intended traffic towards moderator.

#### **4.3.5 *Joining procedure for user invited in online mode***

The Master of one social network is entitled to allow/invite the other users to enter a group and create their appropriate profile which may vary from group to group depending on the settings and applications support in each group. The identification procedure for already registered client say 'B' of MSNP can be defined as

- 1) The invited users would request for security association via the MSNP plug-in or MSNP client application already installed. The user authenticates itself using AuthCert\_B.
- 2) The MSNP will validate the client MSISDN as already registered user. The user request is mapped by database to confirm invitation status by the moderator and lifetime of request.
- 3) The client will be routed to perform GBA based authentication and routing procedure as shown in Fig. 15 to generate new keys and update its SocialCert\_B, containing group and role ID's of the new group.
- 4) The MSNP will update the client status as member of that particular group.

The joining procedure for online invited user that is not already registered with the MSNP would be slightly different and involves following steps:

- 1) The invited user must access MSNP via UE (mobile equipment instead of online-interface) of MSNP to obtain certificates after completing GBA process.
- 2) The user can register to MSNP by the procedure mentioned in Fig. 15 and obtain authentication and signing certificates from PKI.
- 3) The user will repeat from step 2 to onwards for the joining procedure to specific group and obtaining social certificate.

Note: An alternative approach would be to validate the invitation request by MSNP before starting GBA bootstrapping procedure to issue authentication and signing certificate to the new user.

#### **4.3.6 *New group creation by already registered members***

The registered users and MSNP can:

- Securely perform mutual authentication using authentication certificate issued by PKI over HTTPS connection.
- The user (regardless moderator or member) of group can opt to create new group by following the procedure mentioned in Fig. 15. The user and PKI must re-negotiate using GBA procedure to mutually authenticate and fetch session keys for updating the social certificate.
- The MUSS in database for that specific group is updated and the client will store this updated social certificate into its local disk or UICC in case of GBA\_U.

### **4.4 Secure Identification in offline mode**

The offline communication for the MSNP can take following scenarios:

- Both users are registered users of MSNP and hold authentication certificates (AuthCert). Moreover of the two users should be moderator of some social group and willing to invite the other user to join his/her closed group in the offline mode.
- Both of the users have been already registered to the same group in MSNP and want to mutually authenticate each other in the offline mode using client application.

#### **4.4.1 *Offline invitation by moderator to non-registered user of group***

The authentication flow for inviting a new member to MSNP and then client enrollment in MSNP database is depicted in Fig. 17. Suppose user A, who is moderator of group N want to invite user B who is registered user of MSNP for some other social network group. The steps in this procedure can be summarized as

- Both parties will perform mutual authentication as shown in Fig. 17 using ViDP protocol [44] along with AuthCertA and AuthCertB respectively.
- The user A will sign a special purpose "invitation structure", InvStruct\_N (XML encoded) using the public key in SignCert\_A.
- The user A sends the invitation encrypted by MSNP public key containing
  - ID of group N
  - Role\_ID (Assigned role of user within group N)

- Nonce (Time Stamp)
  - SignCert\_A
- The user B must have online communication with the MSNP prior to communicating with other members of the invited social network group to complete registration process and obtain its updated SocialCert\_B from the network operator of MSNP.
  - Next time the user B is online, it authenticates itself with MSNP (using AuthCert\_B) and present InvStruct\_N to MSNP which is checked and verified by the MSNP. Next the MSNP will push user B for GBA bootstrap procedure as defined in 3GPP 33.223 specifications.
  - The PKI will complete GBA bootstrapping procedure with BSF over Ub interface and perform mutual authentication using Zn or Zn-proxy interface.
  - The user is added to the social network N database with specific role defined by user A and social certificate of user B (SocialCert\_B) is updated to include group N with correct status and role of user B.

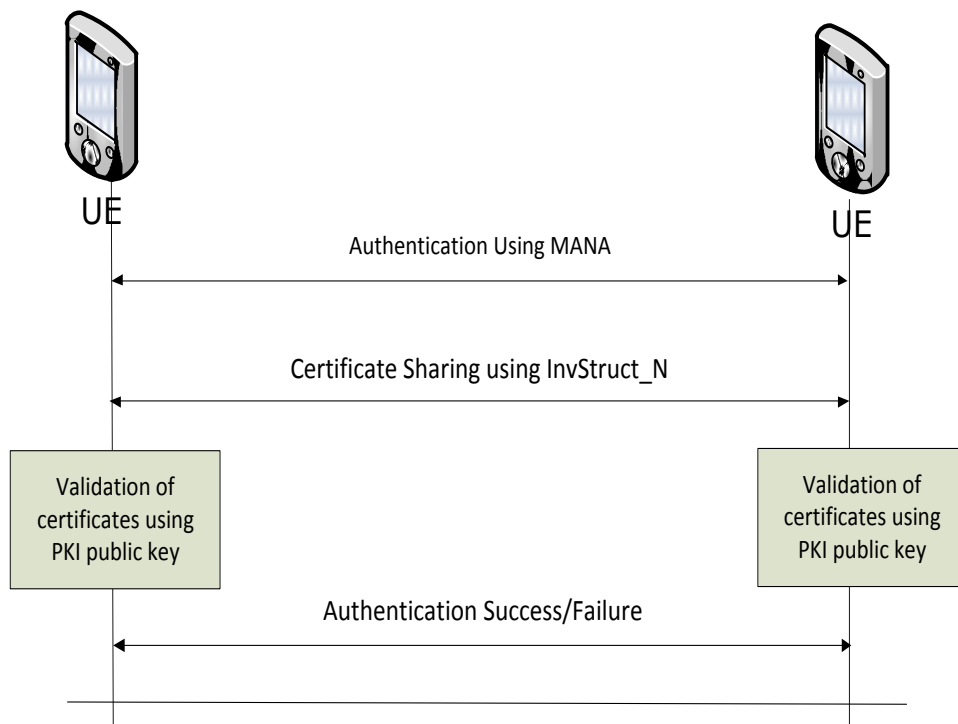


Fig. 17: Offline authentication procedure for non-registered users of particular group

#### **4.4.2    *Offline authentication of users belonging to same group***

The users who are already registered to same mobile social network within MSNP can authenticate each other by the following procedure:

- Both parties will perform initial authentication using corresponding MSNP authentication certificates (AuthCert).
- The users will then use social certificate (SocialCert) for verification and offline connectivity if the other party is part of that particular social group. The social certificate of each user will also determine its role within the group.

### **4.5      Summary**

This chapter provides the solution that successfully encounters all the security requirements and problem definitions described in the previous chapters. The proposed design is fully in-compliance with GAA [3, 6 and 42] standards and related network elements, reference points along with proposed changes are discussed. The proposed design supports both online and the offline modes. The certificates details and their technical specifications are well-defined and the solution is illustrated by using diagrams to show all the steps required for enrollment, registration, authentication and invitation phases. The design is carefully worked out to be flexible for supporting numerous scenarios that are not related with cellular domain but still require secure identification.

## 5 PROTOTYPE IMPLEMENTATION

This section describes in detail about the implementation of secure identification using public, private key pairs and corresponding security certificates based on the solution discussed in previous chapter. The section also provides details about the offline communication and content sharing support among peers using sockets.

Section 5.1 provides the architectural details and the platform used for implementation. Section 5.2 briefly summarizes about the software modules and Application Programming Interfaces (API's) of the functions used in prototype. Section 5.3 provides information about the basic security analysis of the implementation. Section 5.4 provides guidelines for the future implementation based on the outcomes and programming experience of current implementation. Finally, Section 5.5 describes the steps selected for final demonstration of the prototype.

### 5.1 Prototype Structure

The prototype implementation would be termed as thesis prototype in rest of the document and can be classified into online and offline mode. The online mode is primarily the simulation of the modified GBA process illustrated in Section 4.3 of this document. The offline mode is depicting the functionality explained in Section 4.4 of this document.

#### 5.1.1 *Prototype Platform*

The software and hardware requirements can be categorized as:

##### 5.1.1.1 Software Requirements

Application Language:	HTML, CSS, PHP 5.3
Operating System:	Windows, Linux
Protocols:	HTTPS (SSL)
Web Server:	Apache (2.2.11)
Database:	MySQL

##### 5.1.1.2 Hardware Requirements

All the cryptographic keys and certificates requests (CSR's) are generated at client end. The prototype server on the other hand is managing all the corresponding certificates along with its keys, database etc. Following hardware is recommended for the smooth execution of prototype especially at the client end while using 2048 bit RSA keys.

- X86 based Processor (Ideally Pentium Dual Dore or Compatible)
- 512 MB of minimum RAM

- 1GB free space on storage

### 5.1.2 *Prototype Architecture*

The prototype architecture is shown in the diagram below

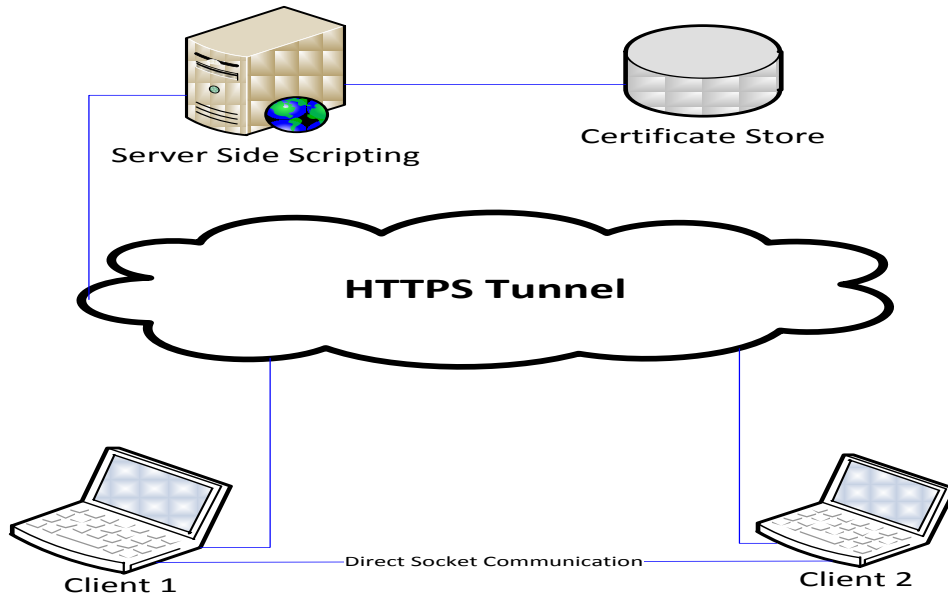


Fig. 18: Prototype Architecture

## 5.2 **Software Modules**

The prototype functionality is primarily based upon two software modules (API's) supported by PHP [53].

### 5.2.1 *PHP Sockets*

According to [53], the PHP socket extension is primarily based on the most widely implemented BSD sockets interface. Although, majority of the functions have the identical names but the arguments differ in many functions.

The Transmission Control Protocol (TCP) was chosen over the User Datagram Protocol (UDP) for client/server communication in offline mode due to its reliability.

### 5.2.2 *PHP OpenSSL Module*

OpenSSL module of the PHP uses OpenSSL [54] functions for confidentiality and integrity of data. The PHP support for OpenSSL is relatively new and quite immature from programmer's point of view.

The key pair generation, Certificate Signing Requests (CSR's), X.509 based certificates, data encryption, decryption, hashing and SSL based communication tunnel is supported by using various functions of this API.

## **5.3 Security Analysis**

The security of thesis prototype primarily depends on the access control mechanism to guard the key and certificate storage both at the client and server end.

### **5.3.1 *Secure Connectivity***

The complete connection setup and subsequent sessions are strongly authenticated and the complete communication is carried out in secure tunnel using SSL. The secure connectivity covers

- User authentication in online mode
- Server authentication by corresponding certificates
- Access authentication in offline mode using ViDP [48]

### **5.3.2 *Potential Attack***

If the attacker is able to get hold of the user private key then it would be able to fabricate and get itself authenticated by the MSNP.

#### **5.3.2.1 Feasibility**

This attack is possible in case of

- GBA\_ME (As key pair is stored on local disk). Hence this attack is valid for the thesis prototype.

This attack is not possible on UICC due to its tamper resistant nature.

## **5.4 MSNP Prototype Recommendations**

The thesis prototype is the initial step towards the successful simulation of the solution proposed in the previous chapter. Hence, the prototype implementation is a mere elaboration of the solution and its practicality for MSNP portal. Thus, the experience learned during implementation may be useful to successfully realize the MSNP prototype. The limitations and recommendations for both offline and online mode are given below

### **5.4.1 *Server Mode***

The thesis prototype assumes that GBA process depicted in Fig. 15 is successfully carried out during registration of the new user and creation of new social group. The MSNP prototype should support all the functionality of GBA bootstrapping procedure. The process of integrating thesis prototype implementation can be achieved by extending it to support basic GBA functionality. One alternative way could be to extend the existing Ericsson GBA API [5] to support the functionality based on the results achieved within this thesis.

### **5.4.2 Client Mode**

The thesis prototype implementation affirms the need of Apache web server for all the clients in order to invoke the functions of the PHP Sockets [55] and PHP module of OpenSSL [56]. In current implementation, the client is an online or offline user accessing MSNP via desktop machine. The future enhancements as per requirements of the MSNP prototype can be divided into online and offline mode.

#### **5.4.2.1 Online Client Mode**

The current implementation is based on a client running Windows/Linux machine along with Apache web server. The real MSNP clients should be the mobile users running mobile based operating system like Android, Symbian etc. Hence the solution can be extended in two ways

- There should be a client application for MSNP that supports the majority of the popular mobile operating system platforms.
- Alternatively, a browser based plug-in can be introduced for all the main mobile based platforms. The plug-in should include functionality of generating keys, CSR's etc

#### **5.4.2.2 Offline Client Mode**

The clients in the thesis prototype interact directly with each other using PHP socket module. In order to successfully communicate, there should be an active network link and the clients should be able to ping each other prior to the connection requests. The MSNP mobile clients should be able to communicate via socket support of the mobile platform or by using Bluetooth. Another option is to implement this direct mode of operation via browser plugin as discussed in the previous section.

#### **5.4.2.3 USIM/ISIM**

The thesis prototype stores the key pairs and corresponding certificates on local storage of the client. This methodology can be followed for GBA\_ME based clients. But in case of GBA\_U, all the credentials should be stored and updated in USIM/ISIM so that the application/plugin should be able to access these credentials.

#### **5.4.2.4 Access Control**

There is no access control mechanism devised for the security of key pairs, certificates etc. stored on the local disk drive. There should be well defined configuration steps to prevent leakage of secure credentials.

## 5.5 Demonstration

The main goal of our demonstration is to illustrate and simulate secure identification between the UE and PKI portal managed by the MNO. The background of our demo includes a fictitious mobile social network MSNP running on server machine with three clients say A, B and C. The clients want to securely register and use MSNP with different roles. The prototype can be classified into five components and these are the available links in prototype left menu.

1. Secure Registration (New users)
2. New Social Group
3. Online Invitation
4. Offline Invitation
5. Offline Authentication

### 5.5.1 *Secure Registration*

The steps involved in secure registration would be elaborated as

1. User A will access the MSNP using the browser and providing the URL of MSNP. The TLS session would be setup between user and the MSNP. The User-A will select ***Secure Registration*** from the left menu. This will open a registration form. The user will provide MSISDN, and fills in other credentials required in the form and will press the submit button.
2. Two public/private key pairs and two certificate requests (csr files) will be generated and all data (including registration details and certificate requests) would be sent to the server. The MSNP will successfully verify that User-A MSISDN is not already registered and would display error message in case of duplication. The MSNP will acquire User-A public keys from certificate requests (csr files) and would sign them using MSNP private key to generate authentication and signing certificates. The MSNP will prompt user to store corresponding authentication and signing certificates. The client would be displayed secure registration completion message.
3. The User-B and User-C would repeat step number 1 to 2 for successfully creating other social groups. The User-B and User-C would sign-out from the prototype.

### 5.5.2 *New Social Group and Online Invitation*

The steps involved in creation of new social group and afterwards inviting other users to the corresponding group would be elaborated as

1. The User-A would click on ***New Social Group*** link and the form will display two fields

- a. Browse option to upload certificate.
  - b. Check-box mentioning new social group
2. The User-A will select check box 'New Social Group' to upload its *signing* certificate and press login button. This will result in popup mentioning that the certificate is invalid. The user will repeat procedure and provide the *authentication* certificate and would be prompted to save its updated social certificate.
3. The User-A will provide unique name for his/her group. MSNP would create social certificate which will include the *Group ID*, *User ID* and *Role ID* (user role within group i.e. moderator, member) of the social group. This file and its hash value would be encrypted using private key of the MSNP. The MSNP will prompt user to store corresponding social certificate.
4. After the successful completion of registration and creating new social group, the User-A would click **Online Invitation** link in the menu. All the registered users would be shown in the grid and A would select User-B and send an invitation for joining his/her social group. The MSNP would update the database about this invitation and generate an e-mail to User-B about this invitation. The User-A would also upload some file at its social network page. The files size should be less than *1MB* and this constraint would be verified during Demo. The User-A would be successfully signed out from the prototype.
5. The User-B would click on **Online Invitation** link and click on 'Join Group' option to authenticate itself using authentication certificate. The form will contain two fields
  - a. Browse option to upload certificate.
  - b. Drop down menu containing names of all social groups.
6. The User-B will select group id of User-A social group and upload its signing certificate and press login button. This will result in popup mentioning that the certificate is invalid. The user will repeat procedure and provide the authentication certificate and would be prompted to save its updated social certificate. The User-B would be successfully logged into User-A social group and would see the file uploaded by User-A during step 4.
7. The User-C would also repeat the step numbers 1 to 3 to create its new social group. Now all three users are registered members of MSNP and User-A and User-C are moderators of their social group. The User-B is not only moderator of his/her social group but also member of social group created by User-A.

### 5.5.3 *Offline Authentication and Invitation*

The steps involved in offline authentication of two MSNP users belonging to different groups without mediation of the server would be elaborated as

The steps involved in offline authentication demo for two users belonging to different groups would be:

1. User-C will click on **Offline Invitation** option on the left menu and then press ready button to accept incoming connection. User-A will also select **Offline Invitation** but would press Connect button. The User-A would be prompted to enter “Hostname” or “IP Address” (or pre-configured in script) in the text box and click “Invite” or “Authenticate” button. The User-A will press “Invite” button.
2. Both users would be displayed the *sum* calculated using ViDP protocol and prompted for verification that the value of sum is same on both sides. After successful verification, User-A will send invitation offer for C to join his/her group say ‘Social\_A’. The User-A will send its invitation vector encrypted by public key of MSNP containing
  - a. ID of B
  - b. ID of N
  - c. Time stamp
  - d. SignCert\_A
3. The User-C will present this vector to MSNP in online mode and would be issued updated social certificate. The User-C would also download the file available at ‘Social\_A’.

The procedure for offline authentication between users of same social network can be:

1. User-B will click on **Offline Authentication** option on the left menu and will click ready button to accept incoming connection. User-A will also select **Offline Authentication** but would select Connect button. The User-A would be prompted to enter “Hostname” or “IP Address” (or preconfigured within script) in the text box and click connect button. The User-A would be prompted to browse and upload the authentication and social certificates (AuthCert\_A, SocialCert\_B) stored on its disk.
2. The User-B would be prompted to receive User-A authentication and social certificate. The User-B will click ‘yes’ and verifies these certificates using public key of MSNP. Upon successful verification the User-B would be displayed successfully validated message. The User-B authentication and

social certificates would be send to User-A and same procedure will be replicated.

## **5.6 Summary**

This chapter depicts the overall structure of the prototype implementation carried out for this particular thesis. Apart of the secure identification design presented in the previous chapter is successfully implemented. The prototype platform, architecture, software modules and API's used during implementation are concisely discussed. The initial security analysis is performed based on the lessons learned during prototype implementation. The verification process is also carried out and thoroughly discussed in the prototype demonstration. Finally, detailed guidelines for future development are presented.

## **6 CONCLUSION AND FUTURE WORK**

### **6.1 Conclusion**

This thesis has highlighted necessary details and understanding about related tools and technologies deployed for mobile social networks and provides in-depth insight toward futuristic emerging trends. The concept of decentralized social networks and the security challenges related to these networks have been thoroughly covered. The research questions outlined in Section 1.3.3 are answered as follows:

1. It has been discovered that there is a vast potential targeting high end customers requiring de-centralized closed social groups with assured security levels. Comprehensive study and research work is carried out to identify these use-cases and detailed analysis is carried out from business and technological point of view.
2. The security requirements identified within this study could pave foundation for successful realization of secure mobile social network portal. The proposed design is in compliance of GAA [3, 6 and 42] standards by fulfilling the security requirements and can be adopted easily with minimal technical requirements. The Network Elements (NE), interfaces, cryptographic parameters and detailed procedures for authentication and key-exchange are also presented in the 3GPP specification format.
3. The architecture for the secure identification to support Mobile Social Network Portal (MSNP) in both offline and online mode is thoroughly covered in Chapter 4. We have chosen the certificate sharing mechanism for performing secure identification and authentication of a user. The device pairing protocol is used for initiating the session in offline mode and gaining trust over the potential compromised network. The certificates details and their technical specifications are well-defined and the solution is illustrated by using diagrams to show the necessary steps required for enrollment, registration, authentication and invitation phases.
4. The design is carefully worked out to be flexible for supporting numerous scenarios that are not related with cellular domain but still require secure identification. The prototype implementation successfully demonstrates this fact and can be independently applied to any application demanding high security in terms of secure registration and authentication.

The proposed identification model and experience learned during implementation have achieved artifacts upon which the succeeding work should be constructed. To sum up, the thesis provides in depth answers to the research questions (section 1.3) and has achieved all the set forth objectives (section 1.4) along with concrete directions for the future work.

## **6.2 Future Work**

This study is the foundational project within SWIN [1] project and thus future work is the most promising aspect of this thesis. Most of the significant research directions for follow-up work have already been covered (section 5.4) including:

- Extension of the Ericsson GBA API [5] to support the proposed design
- Access control mechanism for the secure storage of certificates in case of GBA\_ME

Two interesting dimensions for the future work are the identity management and anonymity protection aspects for the mobile social network portal.

## APPENDIX A

### Screen Shots of Prototype

The home screen of thesis prototype is shown in Figure A. 1. The page provides option for both online and offline authentication and new registration.

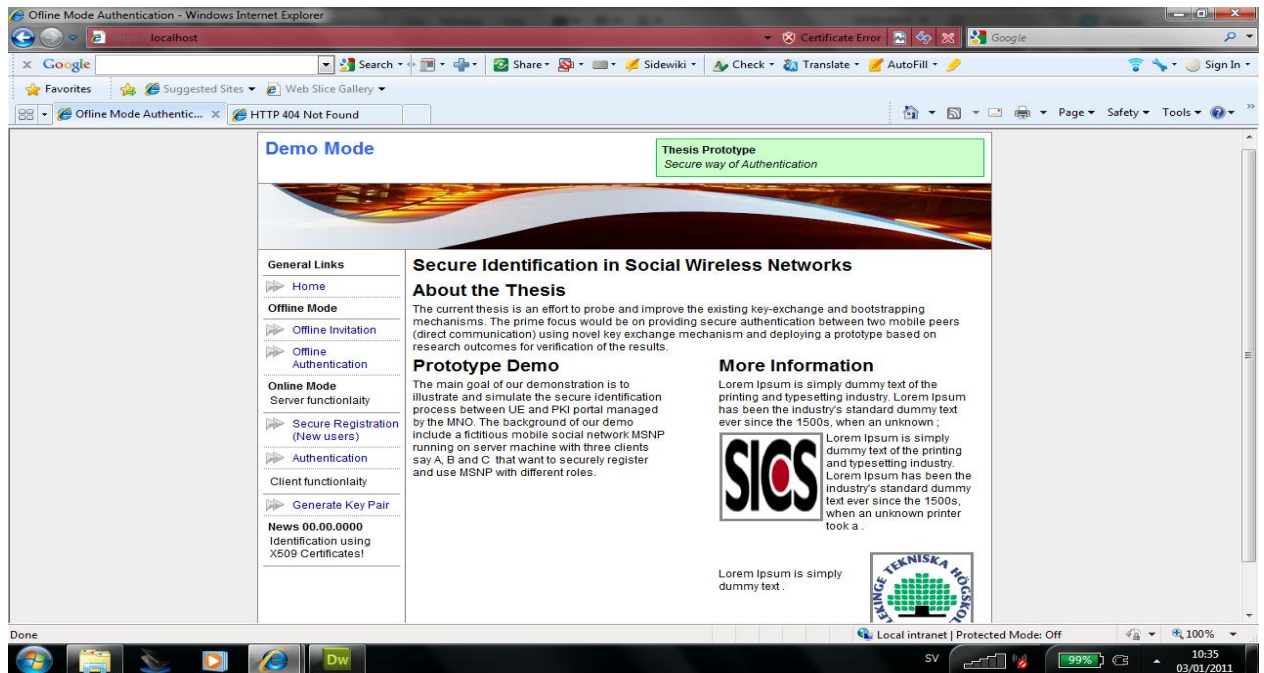


Figure A. 1: Home screen of thesis prototype

#### *Generating Key pair:*

The information necessary for Certificate Signing Request is taken as input from the client as shown in Figure A. 2.

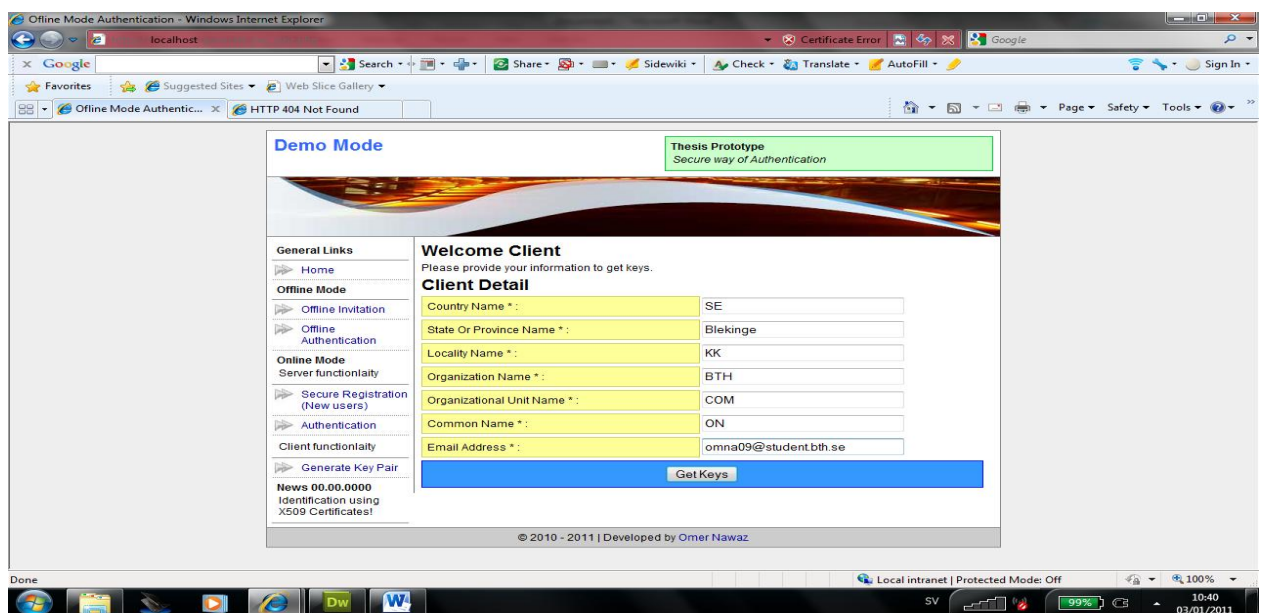


Figure A. 2: Generation of key pairs and certificates signing requests

Public and private key Pairs and their corresponding Certificate Signing Requests (CSR's) are successfully generated as shown in the Figure A. 3.

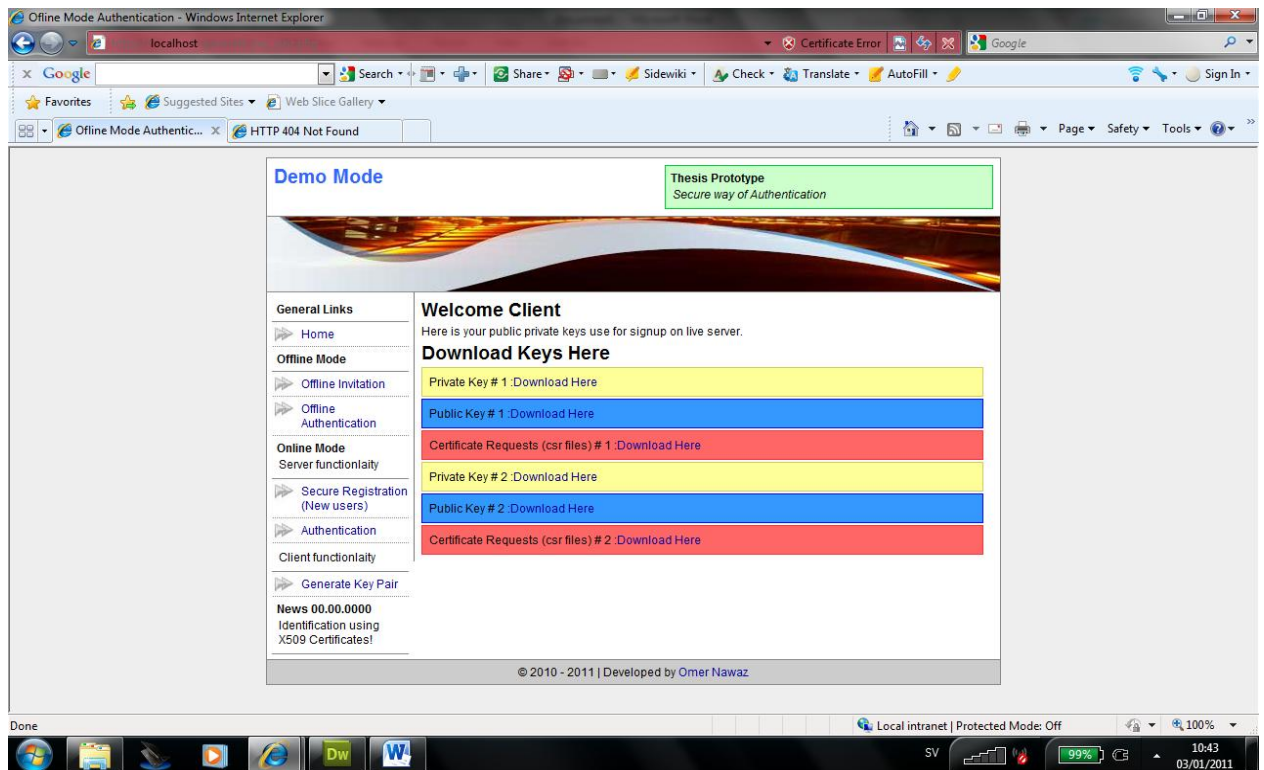


Figure A. 3: Download page for generated credentials

The client can view and validate any of the key pairs and CSR's after clicking the "Download Here" option. The output after clicking the CSR request is shown in the Figure A. 4.

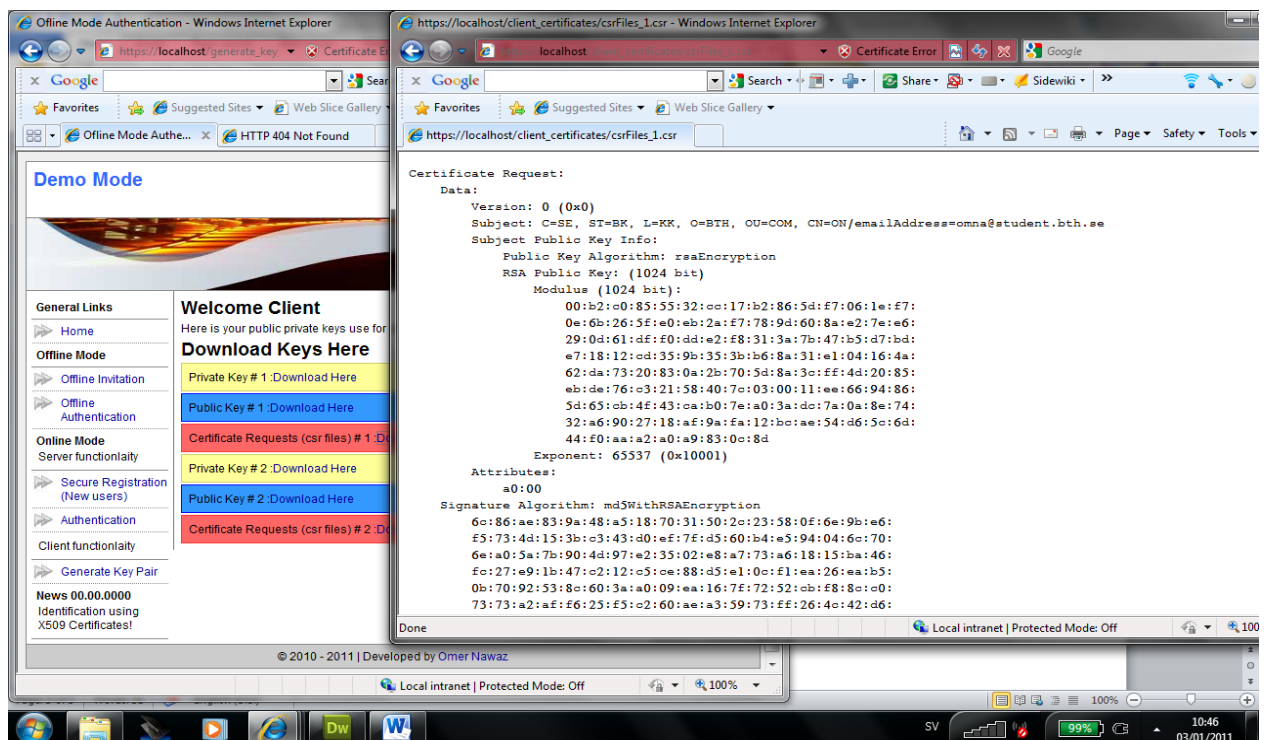


Figure A. 4: Validating certificate request

### Secure Registration Page:

After successful generations of security credentials, the client completes secure registration process using CSR's as shown in the Figure A. 5.

The screenshot shows a web browser window titled "Offline Mode Authentication - Windows Internet Explorer" with the address bar displaying "https://localhost/signup.php". The page has a green header with the text "Secure way of Authentication". On the left, there is a sidebar with a "General Links" menu containing: Home, Offline Mode (with sub-links: Offline Invitation, Offline Authentication), Online Mode (with sub-links: Server functionality, Secure Registration (New users), Authentication, Client functionality, Generate Key Pair), and News (00.00.0000 Identification using X509 Certificates!). The main content area is titled "Signup" and contains the text "Please provide your public key and other information to signup." Below this is a "Client Detail" form with the following fields: Mobile Number \* (123445), Name \* (Omer Nawaz), Address (ABC), Email (on@bth.se), Organization Name, Organization Unit, Zip, City, Country, Certificate Requests (csr files) #1 \* (C:\wamp\www\OfflineMo), and Certificate Requests (csr files) #2 \* (C:\wamp\www\OfflineMo). Each field has a "Browse..." button next to it. At the bottom of the form is a blue "Signup" button. The browser's status bar at the bottom shows "Local intranet | Protected Mode: Off" and the system tray shows the date and time as 10:49 on 03/01/2011.

Figure A. 5: New user registration

The client sends CSR requests to server along with registration information. The server signs CSR with its private key and sends corresponding authentication, signing certificates and the public key of the server. The certificates and keys can be viewed by clicking download here button as shown in the Figure A. 6.

The screenshot shows a web browser window titled "Offline Mode Authentication - Windows Internet Explorer" with the address bar displaying "https://localhost/signup.php". The page has a green header with the text "Thesis Prototype Secure way of Authentication". On the left, there is a sidebar with a "General Links" menu containing: Home, Offline Mode (with sub-links: Offline Invitation, Offline Authentication), Online Mode (with sub-links: Server functionality, Secure Registration (New users), Authentication, Client functionality, Generate Key Pair), and News (00.00.0000 Identification using X509 Certificates!). The main content area is titled "Signup" and contains the text "Please provide your public key and other information to signup." Below this is a blue box with the text "You are successfully signup. Click here to sign". Below the blue box are three yellow boxes: "Authentication certificate :Download Here", "Signing certificate :Download Here", and "Server public key :Download Here". At the bottom of the page is a footer with the text "© 2010 - 2011 | Developed by Omer Nawaz". The browser's status bar at the bottom shows "Local intranet | Protected Mode: Off" and the system tray shows the date and time as 10:56 on 03/01/2011.

Figure A. 6: Validating certificates and server key after secure registration

After completing the secure registration step, the client may sign in to the prototype by using authentication certificate obtained in the previous step. As shown in Figure A. 7, we provided signing certificate instead of the authentication certificate for verification. Subsequently, it successfully provided error that it's not the authentication certificate. The verification is done at server end by extracting the keys from the certificate and validating them with keys stored in the database. The user can also view the server public key as shown in the Figure A. 8.

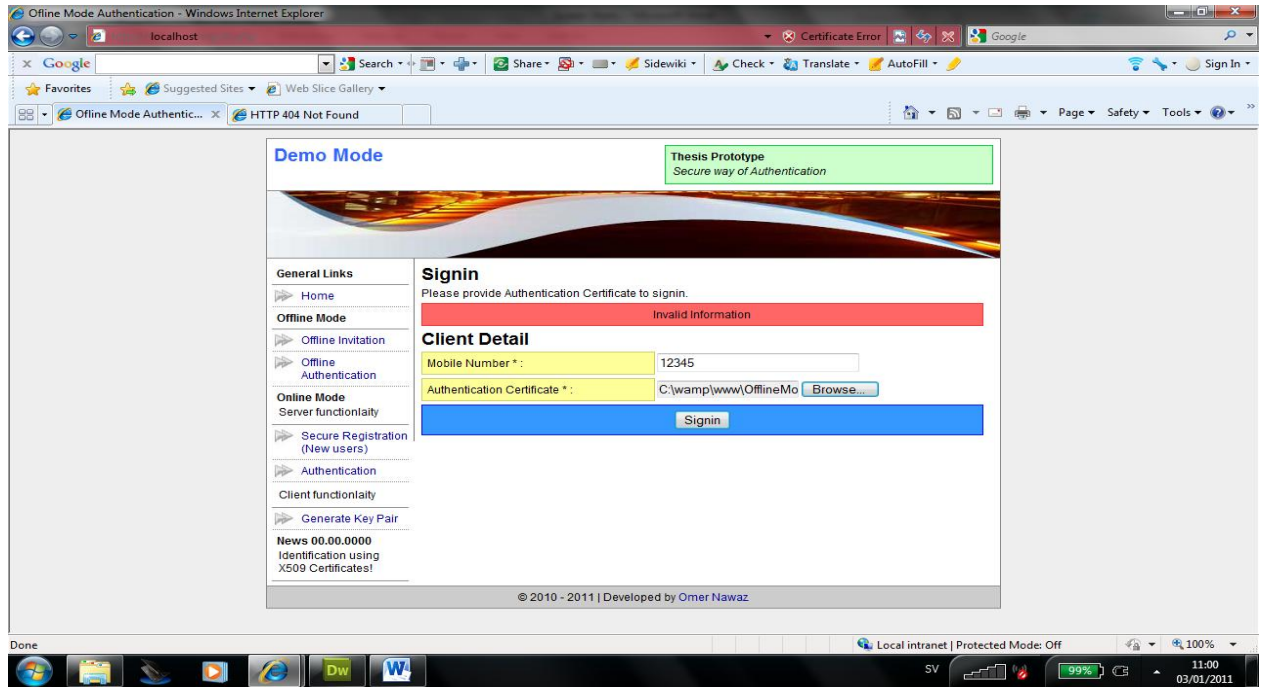


Figure A. 7: Sign in page for registered user

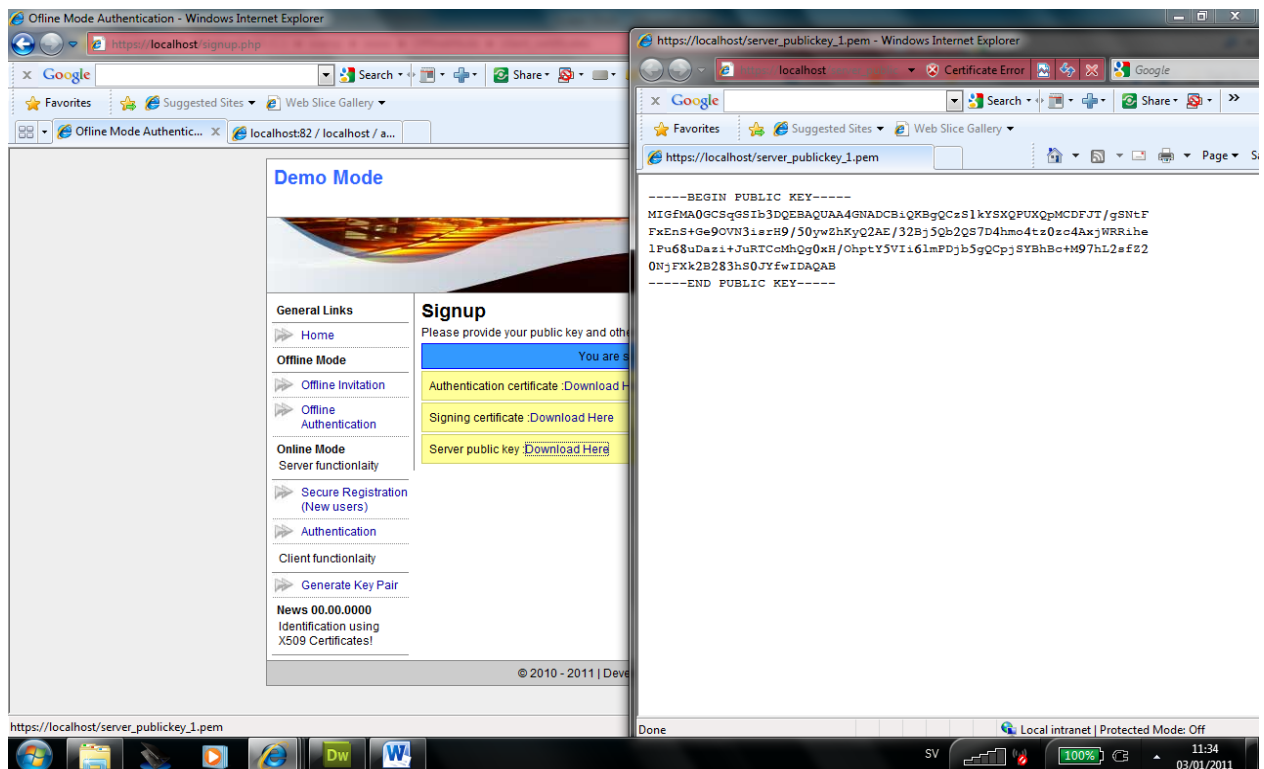


Figure A. 8: View via download option of server public key

After providing correct authentication certificate to the server, the users is authenticated and successfully sign-in to view the “New Social Group” and “Online Invitation” options in the left menu as shown in Figure A. 9.

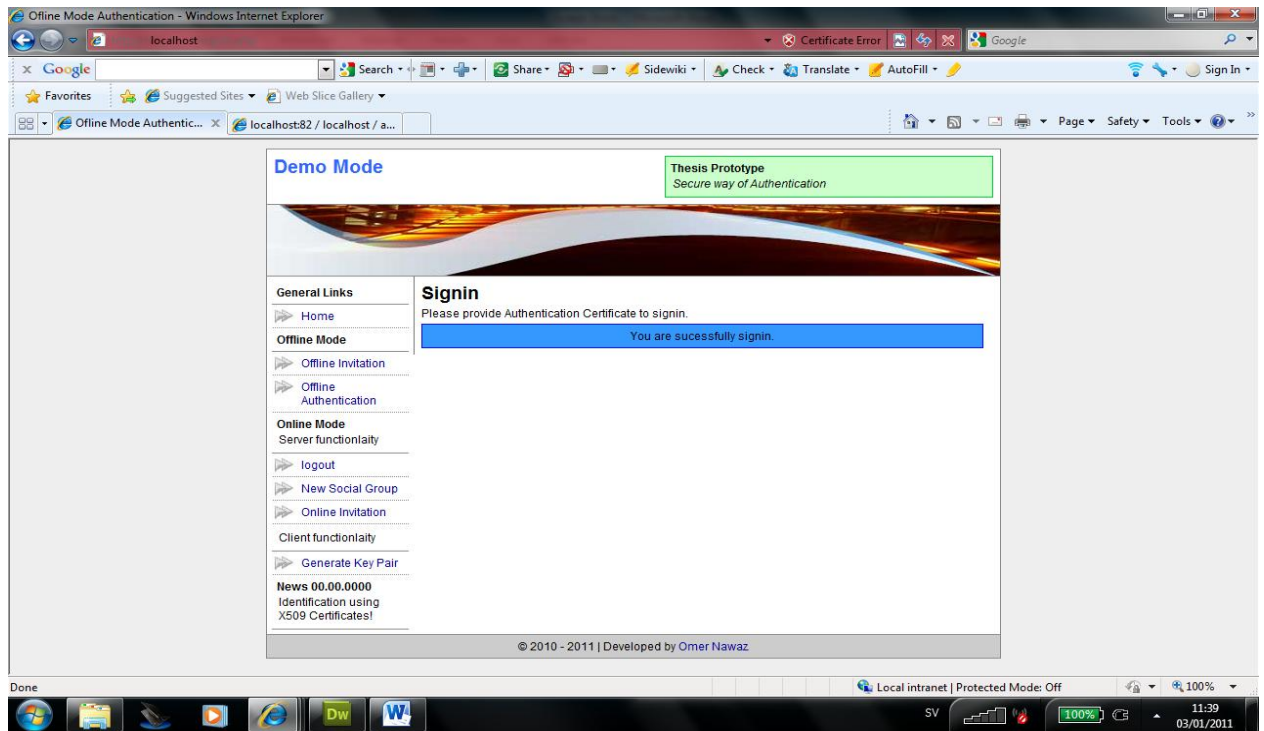


Figure A. 9: Page view after successful login

### ***New Social Group:***

The client will receive his/her first social certificate after this step. The certificate will be updated whenever the clients create a new group or become member of some other social group as shown in the Figure A. 10.

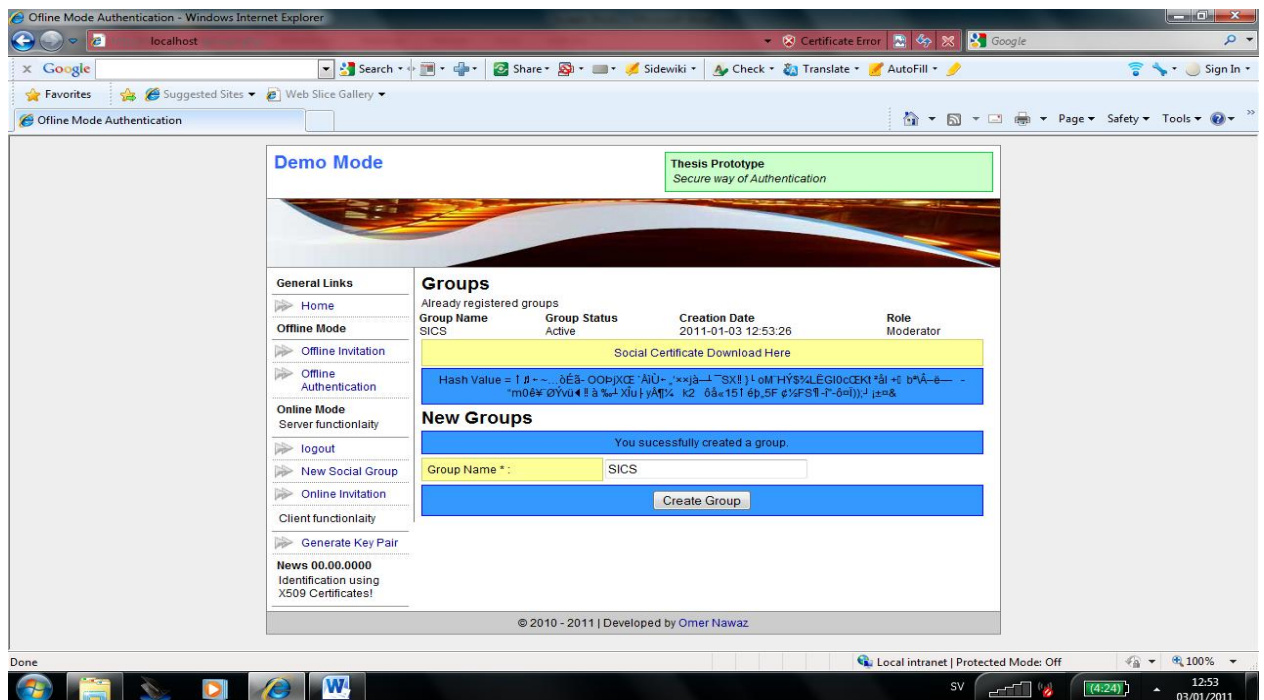


Figure A. 10: Page for creation of new social group

### Online Invitation:

As shown in the Figure A. 11, the online user can view all the registered users of the MSNP. But the client would only be shown those groups where his/her profile is of group moderator.

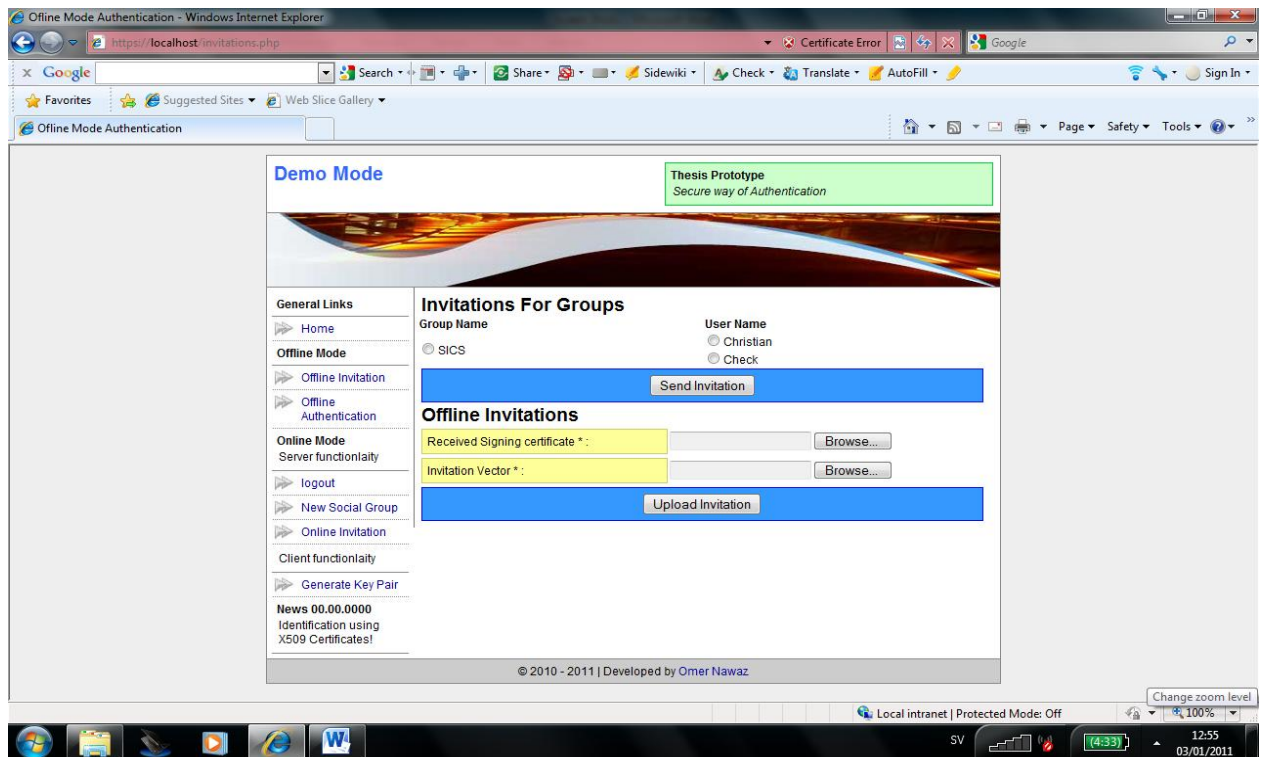


Figure A. 11: Online invitation page

The procedure mentioned above is depicted in the Figure A. 12, as the moderator selects another user from the list and invite him/her to join group SICS.

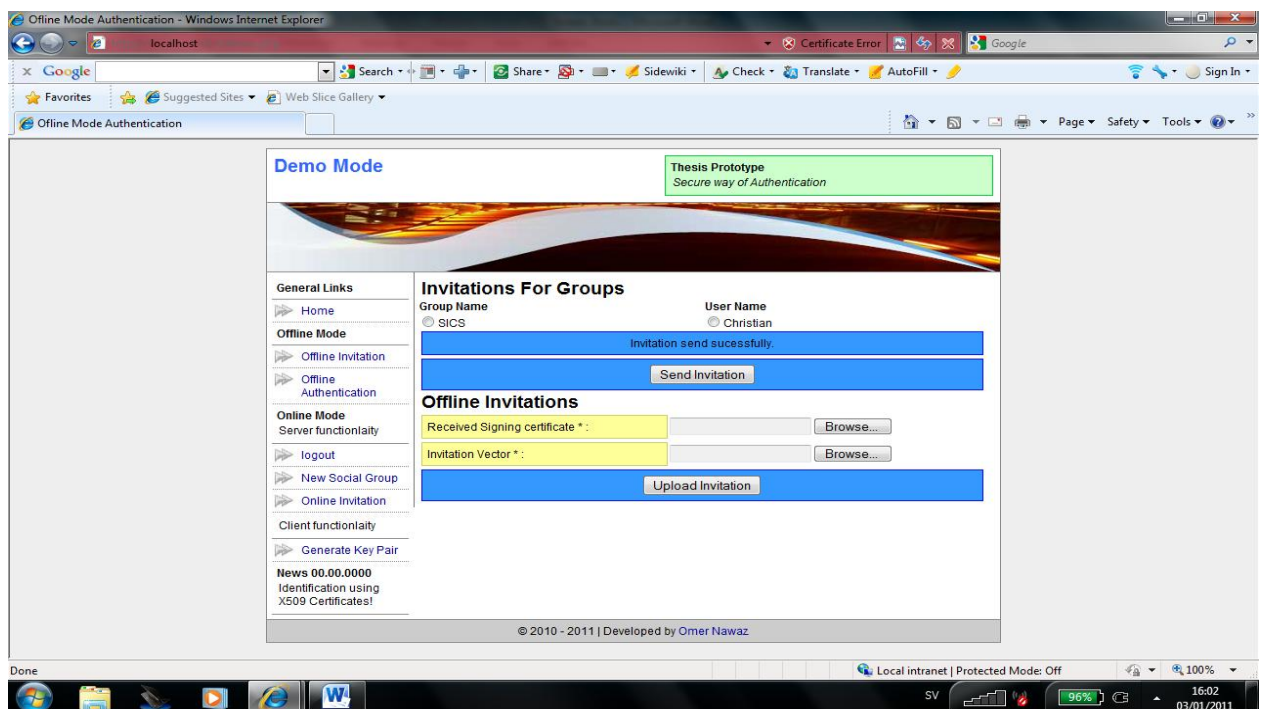


Figure A. 12: Inviting another user to your social group

The invited user can validate the received invitation after logging with its authentication certificate and viewing the online invitation as shown in Figure A. 13.

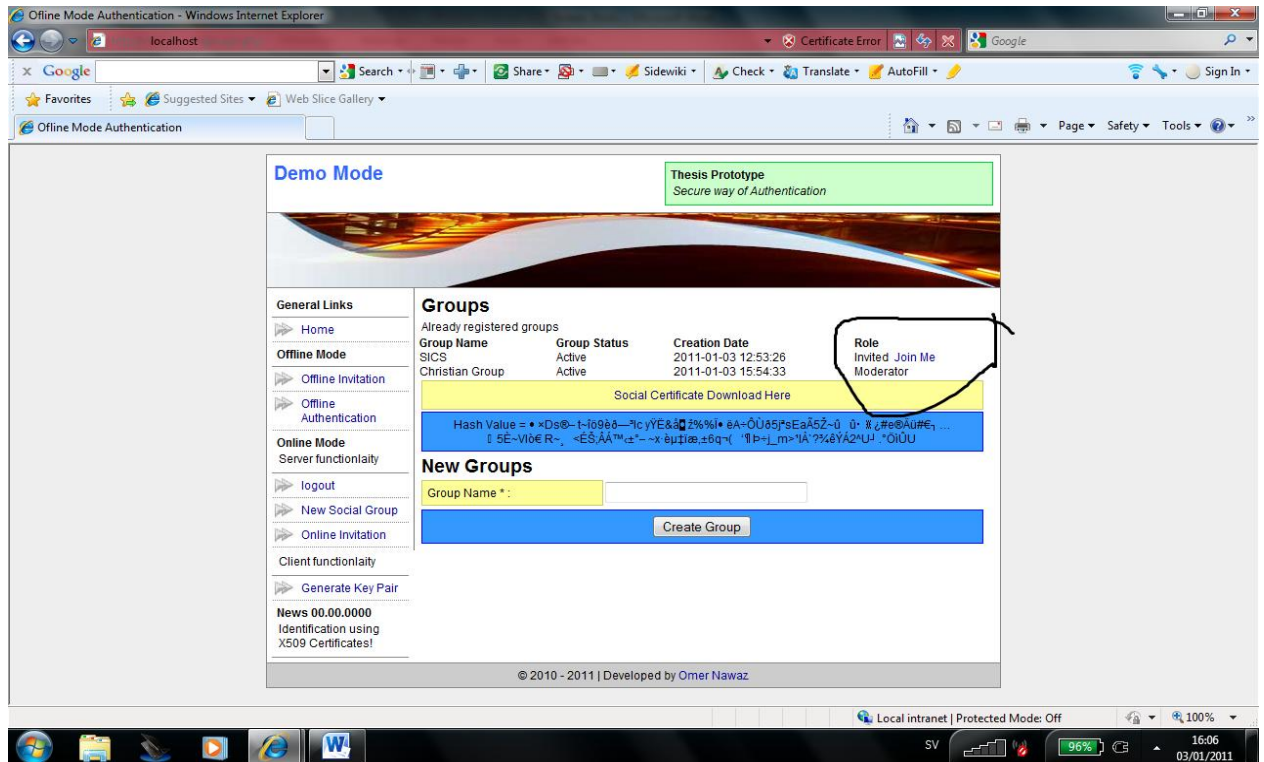


Figure A. 13: Validating online invitation request

### ***Offline Invitation:***

Two registered members of prototype can securely communicate with each other in offline mode using their authentication and signing certificates by using sockets as shown in the Figure A. 14.

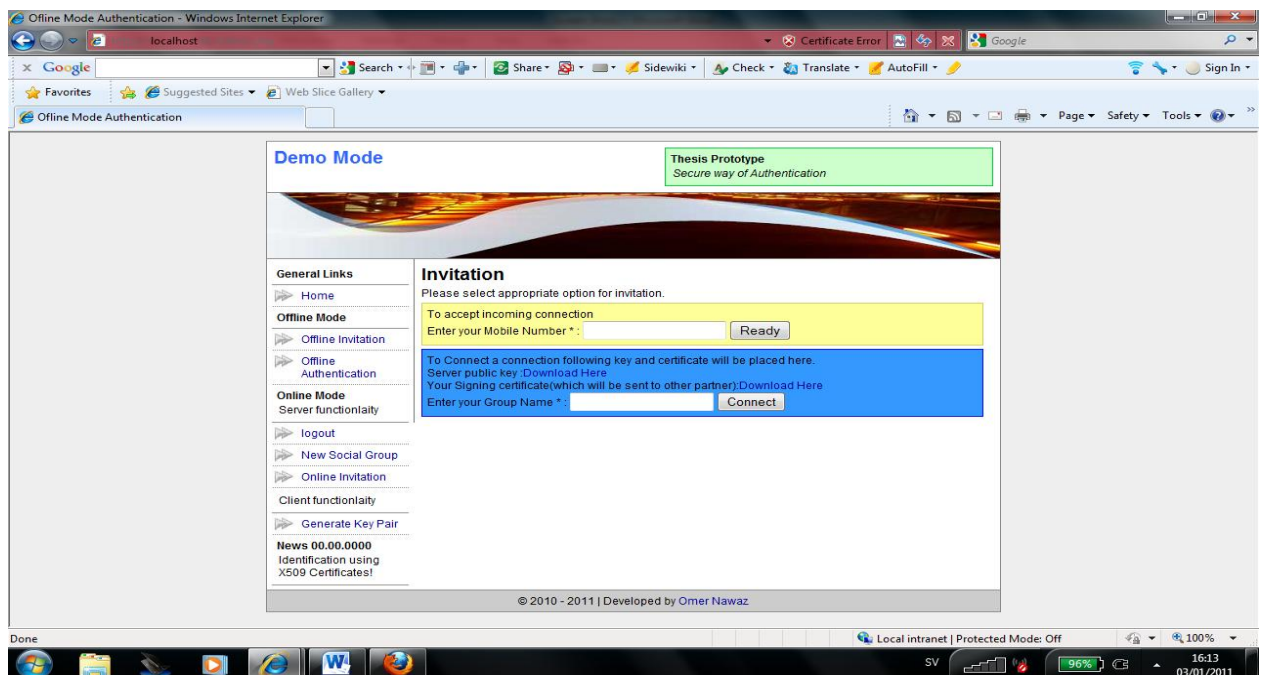


Figure A. 14: Creating offline connection via sockets

The avoid man in the middle attack; the offline communication is secured by implementing the ViDP protocol [48]. As per protocol architecture, both offline clients validate the shared cipher and its sum. Both users must press yes to validate the sum so that the invitation vector and signing certificate for invitation of social group is sent by one user to the other as shown in Figure A. 15.

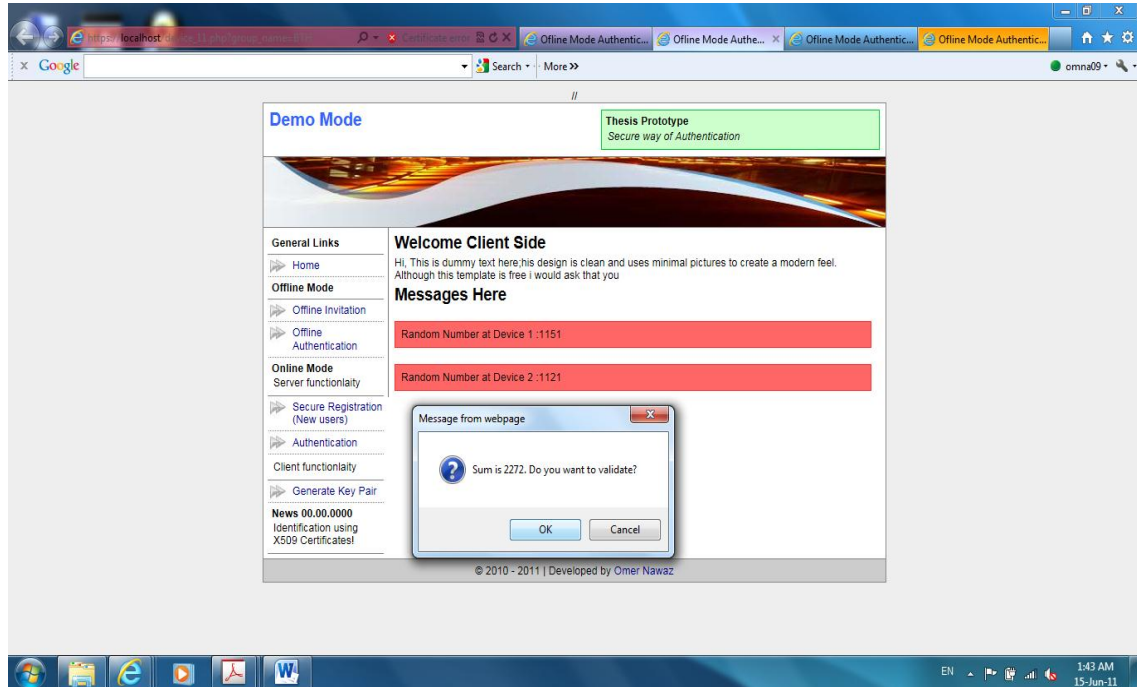


Figure A. 15: Validation of random numbers and sent vector using ViDP protocol

The invited user can download the received security certificate and invitation vector as shown in the Figure A. 16.

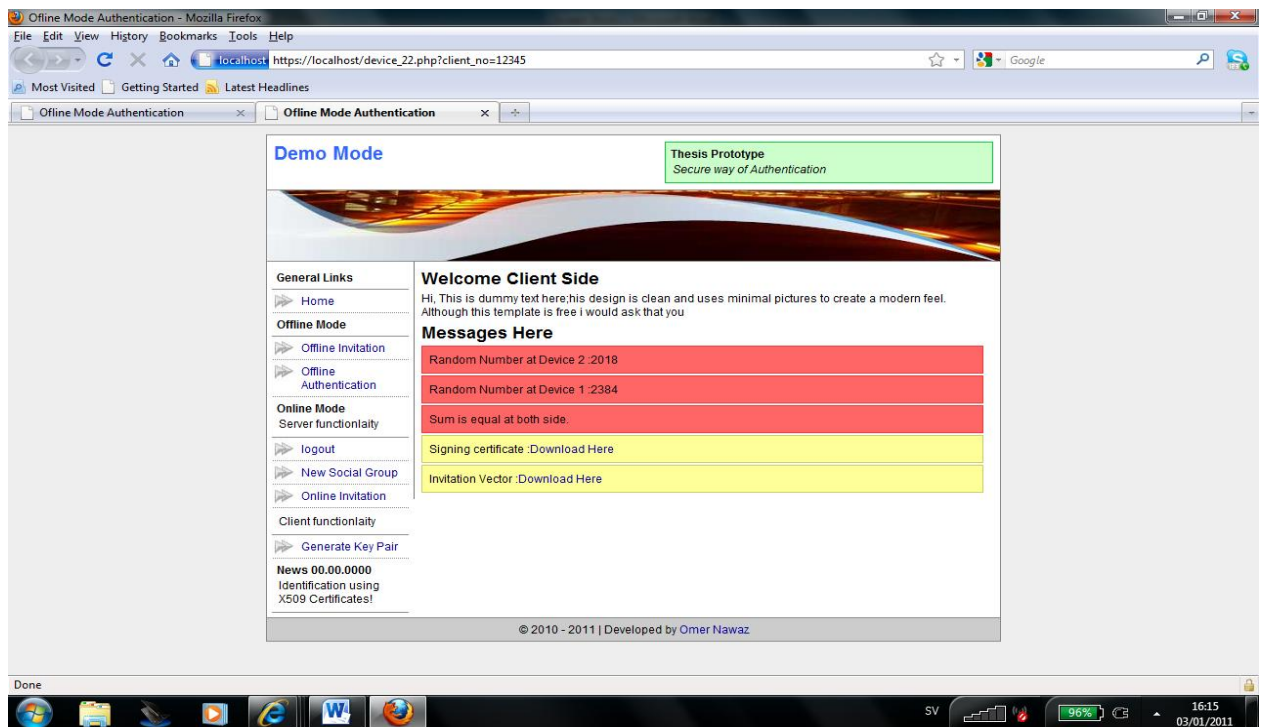


Figure A. 16: Validation of received certificate and invitation vector by other user

The invitation vector received by the invited user is encrypted to avoid tempering for fabricated use as shown in the Figure A. 17.

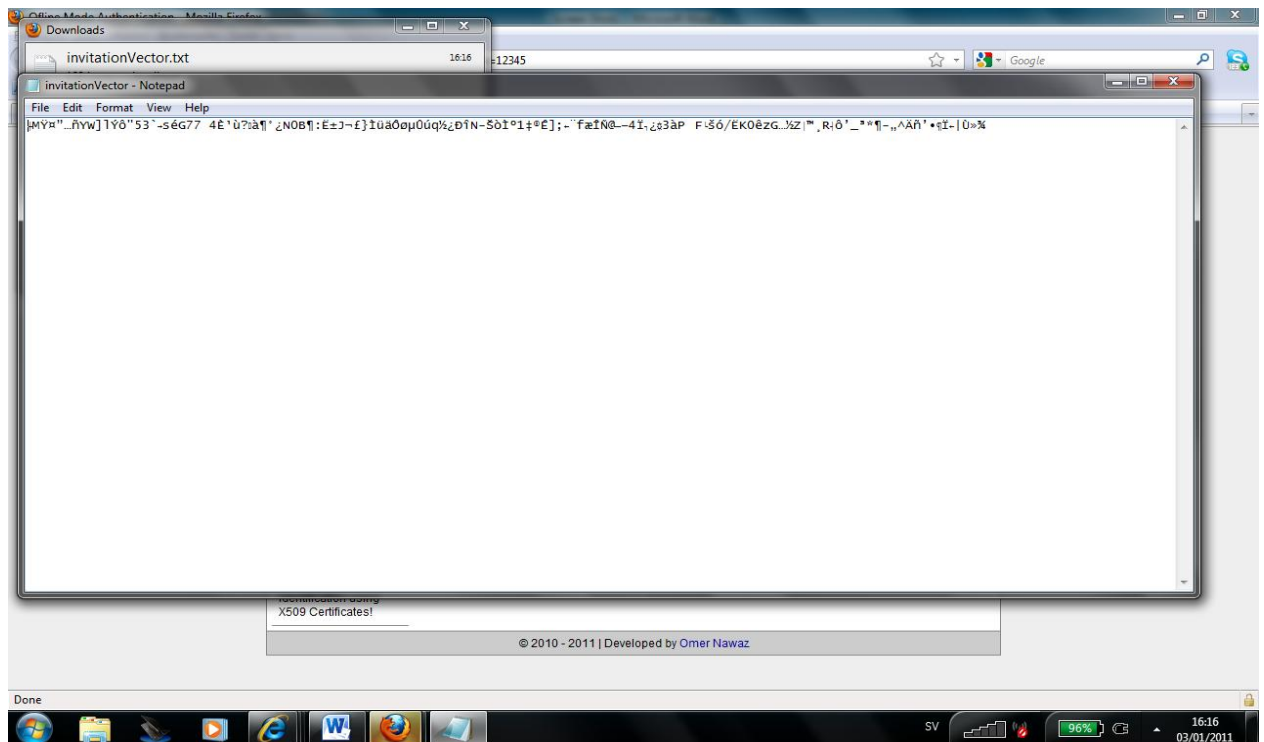


Figure A. 17: Invitation vector in encrypted form

The invited user can go online and present this invitation vector along with signing certificate of the group moderator to join the invited social group. User must upload the received signing certificate and invitation vector as shown in the Figure A. 18.

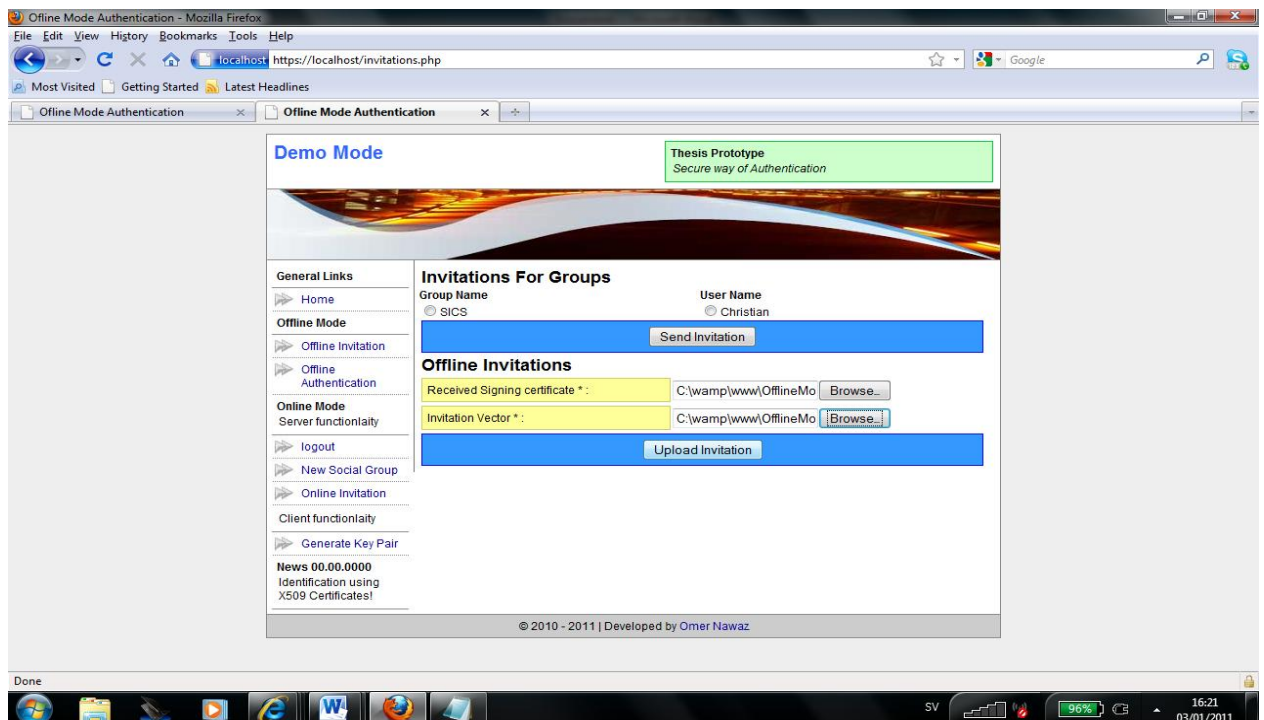


Figure A. 18: Getting online and joining social group via offline invitation

Finally, the user will be successfully enrolled to the group whom invitation was received during offline communication using ViDP [48] via socket interface as shown in the Figure A. 19.

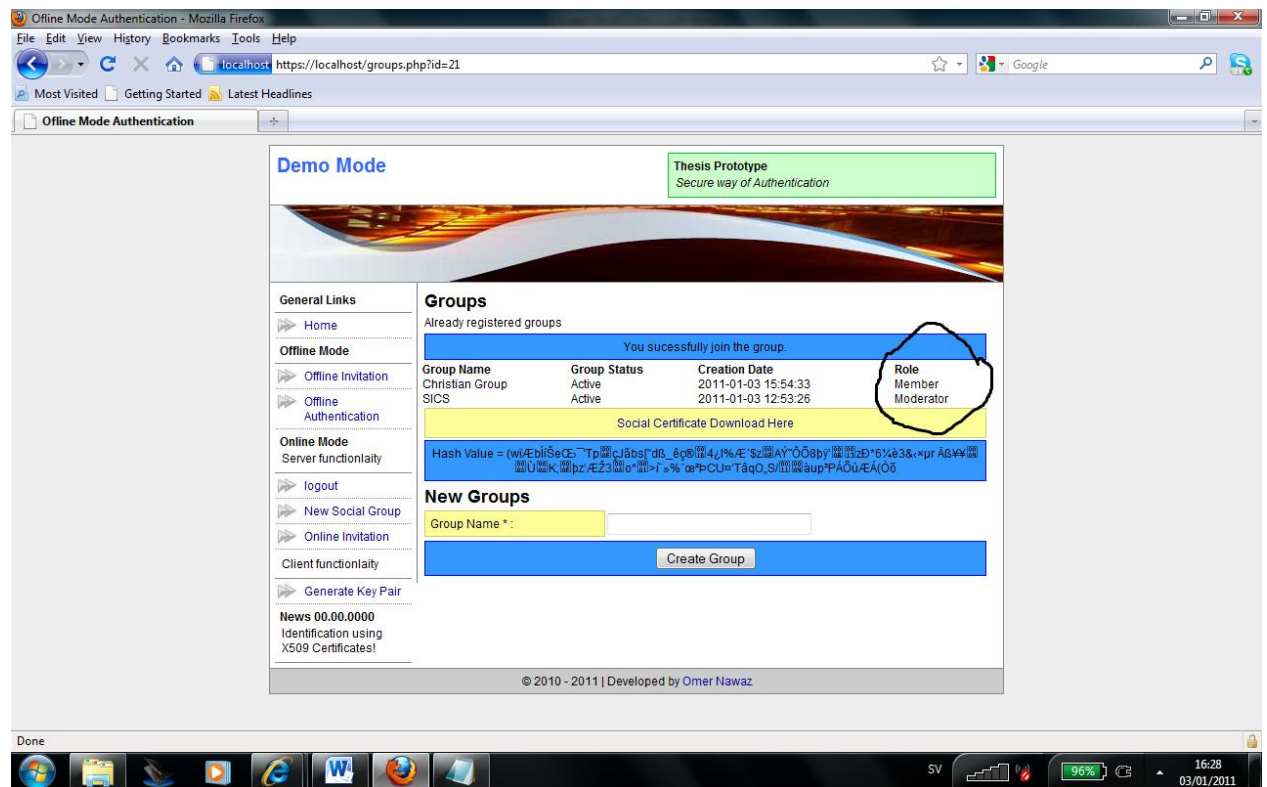


Figure A. 19: Successful membership via credentials received in offline mode

## BIBLIOGRAPHY

- [1] Social Wireless Networks, Secure Identification (SWIN Project), [Online]. Available: <http://www.sics.se/projects/swin>
- [2] Timo Olkkonen, "Generic Authentication Architecture," *Seminar on Network Security at Helsinki University of Technology*, TKK T-110.5290, 2006
- [3] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Generic Authentication Architecture (GAA); System description, version 9.1.0, Release 9, 3GPP, TR 33.919, June 2010.
- [4] Yuh-Min Tseng, "USIM-based EAP-TLS authentication protocol for wireless local area networks," *Computer Standards & Interfaces*, vol. 31, pp. 128-136, 2009
- [5] Ericsson Labs, [Online]. Available: <https://labs.ericsson.com/apis/mobile-web-security-bootstrap/>
- [6] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Generic Authentication Architecture (GAA); Generic bootstrapping architecture, version 9.3.0, Release 9, 3GPP, TS 33.220, June 2010.
- [7] Pew Internet and American Life Project, [Online]. Available: <http://pewresearch.org/pubs/1652/social-relations-online-experts-predict-future>
- [8] OpenID, [Online]. Available: <http://openid.net/>
- [9] Alexa Top 500 Global Sites, [Online]. Available: <http://www.alexa.com/topsites> [Accessed August, 2010]
- [10] myChurch, [Online]. Available: <http://www.mychurch.org/> [Accessed August, 2010]
- [11] Muxlim, [Online]. Available: <http://muxlim.com/> [Accessed August, 2010]
- [12] PartnerUp, [Online]. Available: <http://www.partnerup.com/> [Accessed August, 2010]
- [13] Ryze Business,[Online]. Available: <http://www.ryze.com/> [Accessed August, 2010]
- [14] Ning, [Online]. Available: <http://www.ning.com/> [Accessed August, 2010]
- [15] M.Handley, H. Schulzrinne, E. Schooler and J. Romberg., "Session initiation protocol," IETF RFC 2543, Available: <http://www.ietf.org/rfc/rfc2543.txt> , March 1999
- [16] ITU-T Recommendation H.264, "Advanced video coding for generic audiovisual services," Available: <http://www.itu.int/rec/T-REC-H.264-201003-I/en>
- [17] ITU-T Recommendation H.263, "Video coding for low bitrate communication," Available: <http://www.itu.int/rec/T-REC-H.263-200501-I/en>

- [18] F. Dowsen, D. Stenerson., “Internet Calendaring and Scheduling Core Object Specification (iCalendar),” RFC 2445, Available: <http://www.ietf.org/rfc/rfc2445.txt> , November 1998
- [19] ArticlesBase, [Online]. Available: <http://www.articlesbase.com/internet-articles/history-of-social-networking-websites-1908457.html>
- [20] GIGaom, [Online]. Available: <http://gigaom.com/2010/04/12/mary-meecker-mobile-internet-will-soon-overtake-fixed-internet/>
- [21] GyPSii, [Online]. Available: <http://www.gypsii.com/> [Accessed August, 2010]
- [22] Brightkite, [Online]. Available: <http://brightkite.com/> [Accessed August, 2010]
- [23] Loopt, [Online]. Available: <http://www.loopt.com/> [Accessed August, 2010]
- [24] P. Calhoun et al.,”Diameter Base Protocol,” IETF RFC 3588, Available: <http://www.faqs.org/rfcs/rfc3588.html>, September 2003
- [25] BrightKite Profile at Crunchbase, [Online]. Available: <http://www.crunchbase.com/company/brightkite> [Accessed August, 2010]
- [26] Loopt Profile at CrunchBase, <http://www.crunchbase.com/company/loopt> [Accessed August, 2010]
- [27] I. Chlamtac, M. Conti, J. Liu, “Mobile ad hoc networking: imperatives and challenges,” *Ad Hoc Networks* 1 (1) (2003) 13–64
- [28] L. Venkatraman, D.P. Agrawal, “Strategies for enhancing routing security in protocols for mobile ad hoc networks,” *Journal of Parallel and Distributed computing*, vol. 63, pp. 214-227, 2003
- [29] Rongxing Lu, Zenfo Cao, Licheng Wang, Congkai Sun, “A Secure Routing Protocol with authenticated key exchange for ad hoc networks,” *Computer Standards and Interfaces*, vol. 29, pp. 521-527, 2007.
- [30] M. Jakobsson, K. Sako, R. Impagliazzo, “Designated verifier proofs and their applications,” *Ueli Maurer (Ed.), Advances in Cryptology- EUROCRYPT’96, LNCS*, vol. 1070, pp. 143-154, Springer-Verlag, 1996
- [31] J. Kohl, C. Neuman, “The Kerberos Network Authentication Service (V5),” IETF RFC 1510, Available: <http://www.ietf.org/rfc/rfc1510.txt> , September 1993
- [32] Asad Amir Pirzada and Chris McDonald, “Kerberos Assisted Authentication in Mobile Ad-hoc Networks,” *27<sup>th</sup> Australian Computer Science Conference*, pp. 41-46, 2004
- [33] Nikos Komninos, Dimitrios D. Vergados, Christos Douligeris, “Authentication in a layered security approach for mobile ad hoc networks,” *ELSEVIER computers & security*, Vol. 26, pp. 373-380, 2007

- [34] T. Xu and Y. Cai, "Location anonymity in continuous location-based services," *Proceeding of the 15<sup>th</sup> International Symposium on Advances in Geographic Information Systems (ACM GIS)*, pp. 1-8, 2007
- [35] T. Xu and Y. Cai, "Exploring historical location data for anonymity preservation in location based services." *Proceedings of the IEEE INFOCOM*, pp. 1220-1228, 2008
- [36] Windows CardSpace, [Online]. Available: <http://msdn.microsoft.com/en-us/library/aa480189.aspx>
- [37] VIP, [Online]. Available: <http://www.verisign.com/authentication/> [Accessed August, 2010]
- [38] David Recordon, Drummond Reed, "OpenID 2.0: A Platform for User-Centric Identity Management," *DIM'06*, November 3, 2006, Alexandria, Virginia, USA. Copyright 2006 ACM 1-59593-547-9/06/0011
- [39] Hyun-Kyung Oh, Seung-Hun Jin, "The Security Limitations of SSO in OpenID," *ICACT*, pp. 1608-1611, 2008, ISBN: 978-89-5519-136-3
- [40] HwanJin Lee, InKyung Jeun, Kilsoo Chun, Junghwan Song, "A New Anti-Phishing Method in OpenID," *The Second International Conference on Emerging Security Information, Systems and Technologies*, pp.243-247, IEEE 2008
- [41] A. Niemi, J.Arkkio, V.Torvinen., "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)," IETF RFC 3310, Available: <http://tools.ietf.org/html/rfc3310> , September 2001
- [42] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Generic Authentication Architecture (GAA); Support for subscriber certificates, version 9.1.0, Release 9, 3GPP, TS 33.221, June 2010.
- [43] OMA Security: "Wireless Identity Module," *Part: Security*, version 1.2, 2005
- [44] PKCS #10; *Certification Request Syntax Standard* [Online]. Available FTP: [ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-10/pkcs-10v1\\_7.pdf](ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-10/pkcs-10v1_7.pdf)
- [45] C. Ellison and B. Schneier, "Risks of PKI: Electronic Commerce," *Communications of the ACM*, Vol. 43(2), 2000
- [46] Dwaine E. Clarke, "SPKI/SDSI HTTP Server / Certificate Chain Discovery in SPKI/SDSI," Master thesis in Computer Science and Engineering at MIT (USA), September, 2001.
- [47] C. Gehrman, C. Mitchell, and K. Nyberg, "Manual Authentication for Wireless Devices," *RSA Cryptobytes*, Vol. 7, No. 1, pp. 29-37, 2004
- [48] D. Zisiadis, S. Kopsidas and Leandros Tassioulas, "ViDPsec Visual Device Pairing Security Protocol," *International Conference on Computational Science and Engineering*, Vol. 3, pp.359-364, 2009

- [49] T. Dierks, C. Allen, "The TLS Protocol Version 1.0," IETF RFC 2246, Available: <http://tools.ietf.org/html/rfc2246> , January 1999
- [50] S. Blake-Wilson, M. Nystrom, D. Hopwood, J. Mikkelsen, T. Wright., "Transport Layer Security (TLS) Extensions," IETF RFC 4366, Available: <http://tools.ietf.org/html/rfc4366> , April 2006
- [51] XML Encryption Syntax and Processing, [Online]. Available: <http://www.w3.org/TR/xmlenc-core/>
- [53] PHP Hypertext Preprocessor, [Online]. Available: <http://php.net/>
- [54] The Open Source Toolkit for SSL/TLS, [Online]. Available: <http://www.openssl.org/>
- [55] The Apache, HTTP Server Project, [Online]. Available: <http://httpd.apache.org>
- [56] Open Source Database, [Online]. Available: <http://www.mysql.com>