Privacy considerations for secure identification in social wireless networks

Master's degree thesis

ELENA KOZHEMYAK

Academic supervisor: Sonja Buchegger, KTH
External supervisor: Christian Gehrmann, SICS
Examiner: Johan Håstad, KTH

September 2011

Abstract

This thesis focuses on privacy aspects of identification and key exchange schemes for mobile social networks. In particular, we consider identification schemes that combine wide area mobile communication with short range communication such as Bluetooth, WiFi. The goal of the thesis is to identify possible security threats to personal information of users and to define a framework of security and privacy requirements in the context of mobile social networking. The main focus of the work is on security in closed groups and the procedures of secure registration, identification and invitation of users in mobile social networks. The thesis includes an evaluation of the proposed identification and key exchange schemes and a proposal for a series of modifications that augments its privacy-preserving capabilities. The ultimate design provides secure and effective identity management in the context of, and in respect to, the protection of user identity privacy in mobile social networks.

Keywords: mobile social networks, identity privacy, identity management, pseudonyms.

Sammanfattning

Det här examensarbetet handlar om personlig integritet, identifiering och nyckelutbyte i mobila sociala nätverk. Speciellt adresserar vi dessa aspekter för system som kombinerar mobil kommunikation med kort räckviddskommunikation som Bluetooth och WiFi. Målet med detta arbete är att identifiera möjliga säkerhetshot mot användarinformation och att ta fram ett ramverk för säkerhet och krav på personlig integritet i mobila sociala nätverk. Tyngdpunkten i arbetet ligger på säkerhet i slutna grupper och förfaranden för säker registrering, identifiering och inbjudan av användare i mobila sociala nätverk. I den här rapporten ingår en utvärdering av de föreslagna identifierings- och nyckelutbyteprotokollen, som tagits fram i ett tidigare skede, och förslag till förändringar/förbättringar som förstärker den personliga integriteten. De föreslagna lösningarna ger säker och effektiv identifikation utan att ge avkall på användarens personliga integritet i mobila sociala nätverk.

Nyckelord: mobila sociala nätverk, identitet, säkerhet, personlig integritet, identifikation, pseudonymer.

Acknowledgements

I offer my sincere gratitude to my supervisor at SICS, Docent Christian Gehrmann, whose commitment in guiding me through the whole process was undeniably important to the completion of this thesis. I am appreciative for always finding time for my work and for providing me with inspiration and valuable instructions throughout the whole project. I feel very lucky to have the opportunity to do my thesis within the SWiN project.

I am deeply thankful to my academic supervisor at KTH, Associate Professor Sonja Buchegger, who has supported me throughout the whole work on my thesis. Thank you for all the guidance, help and valuable recommendations regarding my thesis.

I would also like to thank my examiner Johan Håstad who contributed his time to review this thesis.

I am grateful to all members of the SWiN project whose suggestions and comments during the project meetings shaped my work. Your expertise was more than useful in completing all the phases of my work. I would like to particularly thank Ludwig Seitz who contributed his time and efforts in checking and improving my report, and providing me with timely help and feedback.

I thank my colleagues at the Department of Computer and Systems Science in Stockholm University. Thank you for the continuous concern and inspiring support.

I am thankful to my family for the endless love, support and encouragement I have been given, and to all my friends who have been an immense source of supportive and positive energy during these months.

Finally my deepest gratitude goes to Stelios Gisdakis whose unwavering confidence in me always provided me with motivation and strength when times were tough. Thank you for your continued love and support.

To my mother Olga Kozhemyak,
and in memory of my father Sergey Kozhemyak

List of Abbreviations

3GPP	The 3rd Generation Partnership Project
AKA	Authentication and Key Agreement
AP	Authentication Proxy
AV	Authentication Vector
BSF	Bootstrapping Server Function
B-TID	Bootstrapping Transaction Identifier
CA	Certification Authority
CK	Cipher Key
DHT	Distributed Hash Table
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GPS	Global Positioning System
GUSS	GBA User Security Settings
HLR	Home Location Register
HSS	Home Subscriber Server
IK	Integrity Key
IMPU	IP Multimedia Public Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
LBS	Location Based Services
MMS	Miltimedia Message Service
MNO	Mobile Network Operator
MSISDN	Mobile Subscriber Integrated Services Digital Network Number
MSN	Mobile Social Network(-ing)
NAF	Network Application Function
NE	Network Element
OSN	Online Social Network
PKI	Public Key Infrastructure
RA	Registration Authority
SLF	Subscriber Locator Function
SMS	Short Message Service
SNS	Social network(-ing) Site
SSC	Support for Subscriber Certificates
TMSI	Temporary Mobile Subscriber Identity
UICC	Universal Integrated Circuit Card
USS	User Security Settings
UE	User Equipment
VLR	Visitor Location Register
WIM	WAP Identity Module

List of Figures

Contents

Chapter 1

Introduction

The chapter provides a short introduction to the topic of the thesis and the problems which are addressed in the present work. The chapter gives a brief description of the SWiN project which this thesis is a part of and defines the scope of the study.

1.1 SWiN project description

This Master's thesis is a part of the research and development (R&D) project carried out in collaboration between Ericsson, SICS and Sony Ericsson [SIC]. The project addresses the security and privacy issues of identification of users in social wireless networks.

The main initiative of the project is to combine traditional online social networking with direct mode interactions with a particular focus on strong mechanisms for identification and enrolment of users to "closed groups". To exemplify, a "closed group" could be used in an enterprise or business networking context in order to support electronically the interaction among employees within a company. Every member of the group is connected through their personal mobile device such as mobile or smart phone to a special mobile social networking portal which handles document sharing, enables communication by means of instant messaging or blogging etc. The illustrated concept of a "closed group" implies the existence of restrictive and explicit membership rules. The fundamental prerequisite is that only invited members can join the group and every new member must undergo a secure registration and identification procedure before being allowed to join the group. The registration and identification procedure can be triggered by another member or the moderator of the group either through the network or based on direct short-range wireless communication. According to the research direction of the SWiN project, the mobile social networking in closed environments must provide a high level of security to its members through guaranteeing that the following processes are carried out in a secure way [SIC]:

- Secure registration of new users.

- Secure identification and authentication of registered users.
- Secure authentication of group members.
- Secure invitation of new members supported by the existing network infrastructure or through the direct local wireless enrolment procedure carried out between users in close vicinity.

By having as a starting point the described goals, the research project particularly focuses on how to increase the protection of user privacy and personal integrity in mobile social networks. The research project looks into the current secure identification schemes and standardized federation methods and concentrates on the extent to which these methods can be combined in order to provide a strong and scalable identity management framework. It also investigates a series of key exchange methods suitable for creating security associations especially through direct wireless interactions when the network connectivity is unavailable or temporarily lost. The ultimate goal of the research project is the design and security analysis of the novel identification and key exchange schemes though the combination and enhancement of existing schemes. The verification of the proposed methods is done through the implementation of these protocols in a prototype solution that supports a mobile social network portal. The detailed description of the protocols is given in Chapter 4.

1.2 Research area

Mobile devices are becoming more and more ubiquitous. Being excellent tools for social interaction and communication, they extend traditional social networks to mobile space and stimulate a rapid growth of so-called mobile social networks. Nowadays one can easily observe that popular social networks, such as Facebook [Fac11] and Twitter [Twi11], gradually open up new functionality by moving into mobile realm. At the same time, a number of native mobile social networks appear, such as Foursquare [Fou11] and Gowalla [Gow11], which have a focus specifically on mobile use and mobile communication. Mobile social networks hold extended functionality realized by additional mobile technologies, such as short message services (SMS), multimedia message services (MMS), location based services (LBS), etc., and wireless features which include proximity and direct-mode services. The protection of user privacy in mobile social networks becomes an important field of study as it directly affects the acceptance of these services. A special focus of the SWiN project [SIC] is given to the protection of user privacy in the mobile social network by providing effective and secure identity management.

1.3 Research problem

The evolution of mobile social networks has a direction towards more sophisticated ways of communication and interaction between users. On the other hand, it brings new problems to be solved by mobile carriers, mobile manufacturers and service providers. One of the main challenges to secure communication and interaction in social wireless networks is the problem of user privacy protection. According to [CB95], user privacy can be divided into three concepts: identity, location and content privacy. The present thesis addresses the problem of identity privacy protection which is closely related to the problem of strong and secure identification of users due to the fact that sensitive identity information is often transferred during the procedures of user registration, authentication, invitation, etc. In order to protect identity privacy of users and prevent such attacks as identity theft and impersonation, the work proposes a privacy enhancing mechanism to enhance the identity management of the SWiN architecture design for a mobile social network [SIC]. The approach is based on the introduction of user and group pseudonyms which would allow for anonymity. The privacy preserving capability of the mobile social should be increased without affecting the functionality and introducing extra burden to users.

1.4 Research goals

The Master's thesis project has two main objectives. The *first objective* is the security evaluation and analysis of existing identification protocols, and particularly of the novel key exchange identification scheme proposed and implemented within the R&D SWiN project [SIC]. The analysis with a focus on privacy preservation capability is conducted both based on theoretical studies of academic and industry publications and based on results carried out through practical experiments and demonstrations of the novel solution. The *second objective* is to improve the identity management proposed by the initial SWiN design using a pseudonym-based approach and to evaluate the ultimate design to determine the level of protection of personal information of users in the enhanced mobile social network. The goals of the thesis work can be summarized as follows:

1. To carry out an extensive theoretical study divided into major blocks. First, to identify and study major privacy risks, threats and challenges which exist in the mobile social networking context. Second, to study mechanisms and protocols for secure identification and key-exchange mechanisms for mobile social networks, as well as protocols for carrying out secure invitations for interaction based on various approaches, for example, based on physical presence.

2. To prepare an evaluation of the initial SWiN secure identification design [SIC], [Naw11] with special focus on privacy aspects of the design. To identify and

summarize in a problem statement the privacy challenges related with identity management residing in the initial design.

3. To propose modifications and extensions to the identification scheme with a focus on increased identity privacy protection of users by looking closely at identity and group handling procedures. The modifications are based on introducing user and group pseudonyms to prevent the use of real identifiers within the mobile social network.

4. To evaluate the final design that provides secure and effective identity management, while protecting user privacy in mobile social networks.

1.5 Audience

The expected audience of this research includes anyone in the mobile application industry. First of all, the work should attract attention of mobile service providers who are interested in mobile social networking technology and particularly in the development of a new model for mobile social networking with a focus on its application within "closed" user groups. Also, the results of this project should be beneficial to mobile network operators that are eager to introduce to their subscribers new functionality supporting mobile social networks, and of course to mobile manufacturers that plan to develop the "social middleware" in their mobile product devices. Finally, the work also intends to draw the attention of mobile security research community to the novel scheme of identification in mobile social networks that combines traditional online social networking with direct communication services.

1.6 Limitations

The present research work is mainly based on the evaluation of the previously proposed identification scheme for a mobile social network [Naw11] with a focus on the protection of user privacy and personal integrity. The main ambition is to address so called "closed groups", a group of users in close vicinity actively interacting at a specific moment of the time, that implies the existence of restrictive and explicit membership rules. This thesis enumerates modifications and extensions to the current design to optimize the identity management of the design and to improve its privacy preserving capability. The thesis covers identity and group handling with a goal towards the integration of the design with privacy enhancing technologies (pseudonymity mechanisms) while leaving out such concerns as access control, certificate revocation, friend discovery mechanism, etc.
In addition, it is important to highlight that due to university requirements the present document includes a compressed description of the theoretical background (Chapter 3).

1.7 Thesis organization

Chapter 1 introduces the topic and describes the motivation behind the research work. Chapter 2 presents the research methodology used in this thesis. Chapter 3 forms a theoretical background of the thesis. It is based on the profound literature study and gives an overview of important key concepts and protocols mentioned in this work. Chapter 4 describes the initial secure identification design proposed within the SWiN project [SIC]. Chapter 5 forms the problem statement of this thesis. Chapter 6 includes the proposal for modifications to the existing design to provide anonymity to users based on the introduction of user and group pseudonyms. Chapter 7 is the evaluation of the ultimate design. Finally, Chapter 8 includes conclusions and discussion of possible future research directions.

Chapter 2

Research methodology

The chapter describes the research methodology which was used in the thesis project.

The research methodology illustrated on Figure 2.1 has taken a qualitative approach. The qualitative research methods are used for the evaluation of a novel privacy-preserving identification and key exchange protocol [SIC], [Naw11]. The research exhibits why privacy considerations are important for secure identification and authentication of users in social wireless networks and discusses how privacy

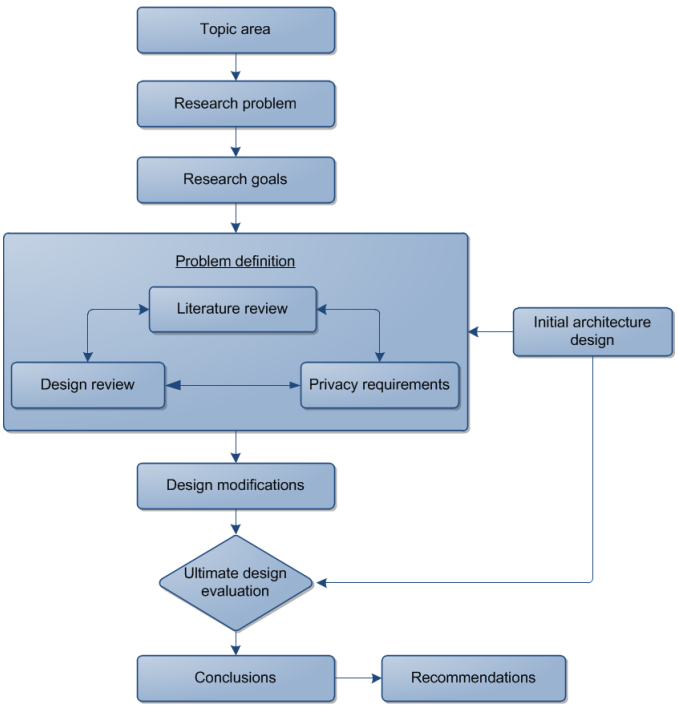


Figure 2.1: Research methodology

and personal integrity of users can be protected in the proposed solution design.

The research starts with a definition of the research topic area and its significance. Selection and formulation of the research problem follows. The research problem creates a number of research goals which are the steps that must be completed in order to archive the research objective of the thesis.

The input to the research process is the initial architecture design of the novel identification and key exchange scheme carried out within the SWiN project [SIC]. The problem definition process consists of three stages. During the first stage, a literature review is done. This embraces a thorough overview of related works conducted within the research topic area during the last years, summary of key concepts and mechanisms necessary to understand the architecture of the proposed solution and a presentation of own reflections on the studied material. This stage forms the theoretical background for carrying out the research. The next stage is a construction of a framework of key security and privacy requirements which should be met in the final version of the architecture design. The construction of the framework is based on the literature studies. The final stage comprises the review of the proposed secure identification design in order to determine a number of possible modifications to the efficiency of the design. Figure 2.1 shows these three stages as interconnected activities because they are not taken step by step but instead are periodically intersecting phases.

The proposal for modifications, based on the defined problem statement, and the evaluation of the updated design is the central part of the research process. The evaluation together with conclusions is the ultimate outcome of the research process. The remaining step of the research methodology is recommendations and proposals for future research directions in the given research topic area.

Reporting of intermediate and final results has been done throughout the whole research process and thus is not mentioned as a separate stage of the research methodology.

Chapter 3

Background

The chapter provides an introduction to mobile social networks and presents key concepts and technology which are used in or relevant to the privacy preserving protocol design specification of which is given in Chapter 4. The chapter starts with a definition of traditional social networks, their types and privacy and security concerns particularly associated with the current move of social networks into mobile space. It covers a description of the secure identification and key exchange standard GAA for secure subscriber identification devices through USIM cards in mobile networks and presents descriptions of several mechanisms for secure device paring using a visual channel.

3.1 Overview of mobile social networks

The global social networking phenomenon is going forward at a steady gait. Most of us are used to start the day with checking the last news by surfing news feeds in favourite social networks. One must admit that social networks became a part of our everyday lives and they completely changed the manner we communicate with each other and the way we spend our time in the Internet. At the same time social networks affected the "online privacy landscape". People who in real life are very unlikely to be more than mere acquaintances may be friends in social networks, sharing information which in real life they would never reveal to each other. But it does not stop here. Social networks increasingly move to mobile space introducing ubiquitous access to services and new ways for social interaction between users. This migration promotes the mobile social networking but inevitably introduces new security and privacy concerns for users who use their mobile communication devices to participate in the mobile social networking. Lately social networks and particularly mobile social networks have formed a popular field of studies and active research area.

Next, an overview of various approaches to privacy analysis in social networks is given, as well as privacy challenges related to the move of social networks into the mobile space are discussed. The section provides a brief analysis on different

architectures of social networks and gives a description of several research projects related to the study. Legal aspects of mobile social networking are also emphasized. Finally, the section provides a summary on major privacy risks and threats in the context of mobile social networking.

3.1.1 Privacy in social networks

To begin with, social network sites are defined as *"web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system"* [BE10]. In case of mobile social networks individuals converse and connect with each other using their mobile devices, such as mobile or smart phones. From the very beginning, the research community draw attention to privacy challenges in social networks. Social networking sites are known to encourage their users to share personal and identity-related information. The information can include such details about a person as their home address, phone number, email address and other attributes, e.g. religion, political affiliations, personal activities, social relations, etc. By examining the pieces of personal information it can be possible to learn enough about an individual and to reconstruct a good picture of the person's identity. If this information is leaked it can lead to an identity theft, personal embarrassment or fraudulent activities against the user. Users tend to believe that only their friends can access their personal information while as a matter of fact the information can be accessible by other entities involved in the SNS, i.e. other non-friend users, third-party advertisers, personal data aggregators or external application providers. If any of these entities do have bad intentions, it leads to privacy risks for the users.

Researchers consider several reasons of privacy risks in social networks. According to [Ros07], social networking sites have introduced new forms of social communication processes which as a result changed the social behaviour of people who use these networks. Often people disclose pieces of personal information either while being unaware of doing it or while being unconcerned or unfamiliar with the consequences that it could entail. The paper also highlights that privacy control mechanisms are often inadequate and lack flexibility and ease of use.

The work [ZSZF10] provides a thorough analysis of privacy conflicts that may exist in SNS. The authors create a special framework for assessing security and privacy of an online social networks (OSN) based on the analysis of common OSN functionalities and existing architecture types for social networking (i.e. client-server versus P2P architecture). The authors conclude that design conflicts emerge in the collision between security and privacy concerns on the one hand and the original goals of OSNs, namely usability and sociability, on the other hand [ZSZF10].

The study [KW08] focuses particularly on the flow of information that exists among social networking sites, third-party servers, external applications and other web sites. In the context of the study the authors perform two experiments that show that 1) social networks tend to have quite permissive default privacy settings

and 2) the use of third-party domains by popular social networks is high. The former can be exemplified by saying that when a new user registers in Facebook certain default privacy settings are enabled. For example, "Public search" (allows the user's profile to appear in search engine results) and "Instant personalization" (displays the user's activity on partner websites to the user's friends who visit these sites) are turned on by default [weba]. The later underlines the pervasive tracking of user activity by third-party domains. Facing these facts, the authors define the privacy problem as the problem of appropriate access to the information. There is a lack of awareness among users regarding who has access to their personal information and what information exactly is shared. The authors thus enumerate so-called privacy bits (pieces of personal information, namely a thumbnail profile, greater profile, list of friends, user generated content and comments) and create a mechanism to define the *bare minimum* of private information which is needed for a particular interaction [KW08]. For example, if an external application requires more than the default set of privacy bits for interaction then the user is notified and the user decides if the application is allowed to access the information requested in excess of the allowable privacy bits and optionally set the duration if access is granted. The described solution can be implemented as a web browser extension.

A number of works discuss privacy practices and policies in social networks. The work [BP09] provides a comprehensive evaluation of security and privacy policies of a selection of social networking sites using a set of outlined criteria. The authors bring up a discussion about the incompatibility problems with mobile web browsers and mobile devices which have a bad effect on privacy practices. The main conclusion of this work is that providers of social networking services still fail in providing the users with sufficient privacy control and regulating the dynamics of privacy in social networks. The work defines "the increasing privacy salience phenomenon" as an urgent need for increasing privacy protection of users and raising privacy awareness among them. Finally, the authors underline that it is important to promote privacy by offering clear and user-friendly interfaces of the services so that users can explicitly see what personal information they share and what parties have access to it.

A number of researchers try to define and improve privacy protection in existing popular online social networks. For example, NOYB [GTF08] is an approach which can be implemented into existing social networks, e.g. Facebook [Fac11], through installing a special web browser plug in. The method preserves user privacy by means of partitioning private information of a user into atoms, then encrypting each atom of information and finally substituting it with another user's atom from the same class of atoms. Substitution is done pseudo-randomly by selecting an atom which index is the index of the initial user's atom encrypted using the symmetric key. A special key management protocol distributes keys to only authorized users who are allowed to view private information. For example, assume that a social network stores the following four pieces of information about each registered user: name, sex, age, home town. Consider that Alice's profile information is partitioned into two atoms *(Alice, female)* and *(20, London)*. The atoms are first encrypted

and then are substituted with atoms that correspondingly belong to users Bob and Carol. In the end, Alice's profile would look like *(Bob, male)* and *(19, New York)* and only authorized users, e.g. Alice's friends, would be able to reverse encrypting and retrieve real user information. However, while this approach protects the private data of user, it does not protect relation links between users.

3.1.2 Social networking architectures

While some researchers strive to improve privacy protection in existing popular social networks built in a centralized way, others study architectures of social networks and focus on introducing new models to embed user privacy protection in the design. Several recent papers are dedicated to analysis of social network architecture as a topology of the underlying network components.

The ultimate goal of PeerSon [BSVD09], Safebook [CMS10] and Diaspora [SGSZ] projects is to create a light-weighed privacy-preserving distributed platform for social networking. The solutions prevent privacy violations and ensure privacy protection of users. The distributed approach makes it possible to create a self-organized, decentralized and at the same time scalable social networks, as well as helps to mitigate several privacy problems, for example to reduce the risk of compromising and exploiting for monetary revenue the user information which is stored centrally in traditional client-server social networks.

PeerSon project

The PeerSon project [BSVD09] proposes a peer-to-peer (P2P) infrastructure for privacy-preserving social network. The project applies the P2P approach in order to replace the centralized authority that exists in traditional online social networking. The PeerSoN approach is enhanced with encryption and access control mechanisms which aim to solve the privacy problem related with the weak protection of user data against access by unintended entities such as providers of OSNs, third-party advertisers or external applications providers. In PeerSoN users can encrypt their personal information and content as well as control who has access to it. The system implies the existence of an adequate key sharing and distribution mechanisms. The system also supports direct communication between peers (to be precise between devices which peers use to communicate) to enable communication during the periods when Internet connectivity is temporarily lost or unavailable, i.e. enabling delay-tolerant networking. To summarize, the PeerSon approach is based on three key principles: decentralization, encryption and direct data exchange.

In order to identify peers in the network each peer must have a unique identifier. The authors propose to use either the hashed value of the user's email address or to use the public key as a GUID (Global Unique identifier). The main assumption of the PeerSoN approach is the availability of a PKI which provides a means to distribute public keys in the network, to verify and revoke them. At the moment the project members work on reducing this assumption.

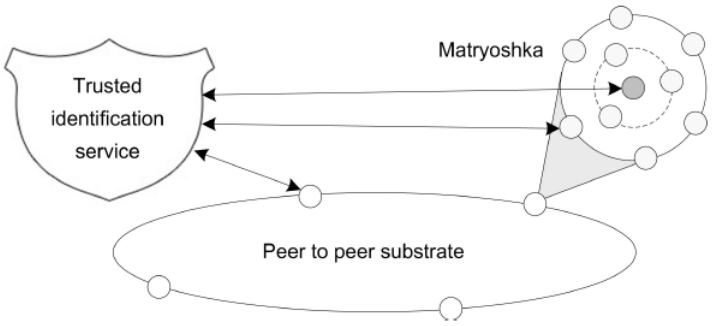


Figure 3.1: Three components of Safebook [CMS10].

Safebook project

Safebook [CMS10] is another attempt to create a distributed P2P social network. The research group proposes a solution which is based on three architectural components: a trusted identification service, a peer-to-peer substrate and so called matryoshkas. The trusted identification service enables authentication and provides a unique identifier to each user of Safebook. The P2P substrate consists of all the nodes of the network and provides a decentralized global data access or in other words lookup service. Finally, matryoshkas are special structures which provide end-to-end confidentiality and enable distributed data storage with privacy preservation. The matryoshka structure is created for each user. The user is the core of the matryoshka and shells of the matryoshka denote the layers of trust and contain nodes of trusted contacts. The nested shells of a matryoshka structure thus provide hop-by-hop trust model. Only trusted contacts of the user can reveal the identity of the user and link the IP address to the user identifier. The fundamental assumption of this approach is the trust relationship between peers and trust placed in the identification service. Figure 3.1 demonstrates the basic components of Safebook architecture and communication links between them.

Diaspora project

Diaspora project [SGSZ] has a status of a proposal and is currently under development by a group of students at New York University's Courant Institute of Mathematical Science. At the moment, not many details about the technical specification of the approach are available.Diaspora is positioned as an open, privacy aware and personally-controlled social network. The idea of the approach is that all the content of a user remains on the personal server which the user runs (for example, on the personal computer). Thus, all the content belongs to the user and is personally controlled by them. In a nutshell, Diaspora provides a way for a user to set up their own server ("Pod"). A "Pod" can host a number of Diaspora accounts ("Seeds"). The user can create and manage multiple "Aspects" within a

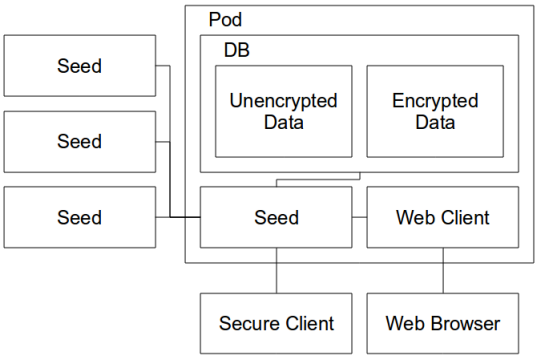


Figure 3.2: The architecture of Diaspora [Wik].

"Seed". "Aspects" are in fact groups of the user's friends defined by the user. The concept of "Aspects" is similar to the concept of groups, for example in Facebook. If user A assigns user B to Aspect X then user B can only view the content of user A available to Aspect X. Users on different seeds can interact and share any social data such as updates, status messages, pictures or videos. According to the security model of the approach, users are given the control of who can access their content and all communication including the message traffic is encrypted with a symmetric key. Three different levels of security are defined as *None* (posts are not encrypted and available to anyone), *Low* (posts are encrypted on request)and *High* (all posts are encrypted) [Wik].

Figure 3.2 is a diagram that demonstrates the architecture of Diaspora. Here Web Client is an HTTP interface built into pods which allows users to easily connect to their seeds remotely from anywhere. Secure Client is an alternative to the Web Client and allows advanced secure communication.

Encryption of posts within an aspect (group of users) is done according to the following scheme [Wik]:

1. a random key (RK) is generated for the aspect
2. the post is encrypted with the random key: enc(RK, msg)
3. for each recipient Rn, RK is encrypted with their public key: enc(pub(Rn), RK)
4. the encrypted key is sent to each recipient

In this scheme however is not clear what happens in case a friend joins or leaves a group and how the problem of backward and forward confidentiality is solved.

Nevertheless the distributed manner of social networks remains the biggest challenge for these projects to deal with. In particular, the challenges of P2P social are

outlined in [BD09] and mainly include questions regarding the storage of data, synchronization mechanisms, topology structure, search mechanisms, integration with other sites and applications, security, connectivity and other issues related with P2P nature of social networks, etc.

As it is discussed later in Chapter 4, the architecture for the mobile social network proposed within the SWiN project combines both centralized and decentralized approaches to social networking. On the one hand, such procedures as user registration and group invitation activation are done centrally, by the Mobile Social Network Portal being a central authority. On the other hand, users of the mobile social network should be able to interact with each other even when the connection to the central portal is unavailable. For example, users should be able to invite each other to groups, i.e. issue and transfer group invitations, through direct mode communication like Bluetooth, WiFi or NFC. The study of the projects listed above is important to understand the problems related with each approach to build a social network, be it centralized or decentralized. Key sharing mechanisms, encryption schemes and user identity choice mentioned above are also among the challenges to be solved by the members of the SWiN.

3.1.3 Ubiquitous mobile computing

The mobile Internet becomes ubiquitous rendering applications like social networking anywhere, any time and with any device. Today (as of August 2011) the total number of active users in Facebook is 500 million [webb]. Below is the extract from Facebook statistics page which has a separate section about the mobile users of Facebook:

- *There are more than 250 million active users currently accessing Facebook through their mobile devices.*
- *People that use Facebook on their mobile devices are twice as active on Facebook than non-mobile users.*
- *There are more than 200 mobile operators in 60 countries working to deploy and promote Facebook mobile products.*

The above mentioned facts mark the popularity growth of mobile social networks and their use among users. Nowadays one can easily observe that such top social networking sites like Facebook [Fac11] and Twitter [Twi11] gradually open up new functionality by moving into mobile realm. The major task of these sites is to catch up with developing and improving functionality of social networking services in order to adapt them for the access and use by means of mobile devices. At the same time, a number of native mobile social networks appear, such as Foursquare [Fou11] and Gowalla [Gow11], which focus specifically on mobile use and mobile communication.

3.1.4 Towards mobile social networks

This section describes a number of models which were proposed for mobile social networking at different times. Many of these mobile social networks applications gained success and wide popularity among users of mobile and smart phones and support from industry.

Dodgeball mobile social network

It is worth starting from the beginning of mobile social networking. One of the first mobile social networks was Dodgeball founded in 2000 by Dennis Crowley in the United States, then later on acquired by Google in 2005, and finally replaced with Google Latitude in 2009 [Tim]. Dodgeball was a pioneering project but it was not a GPS-based mobile social network. Instead, a user could "check-in" by means of sending short text messages with the current location to the central Dodgeball service which then could distribute this information among the user's friends by sending out notification text messages. More details about it can be found in the case study [Hum07].

Serendipity project

In 2004 a group of researchers at MIT Media Lab proposed to mobilize the social software by introducing an infrastructure that combined the existing mobile communication with the wireless connectivity functionality of mobile devices, e.g. Bluetooth [EP05]. The idea of Serendipity project was to facilitate the interaction between physically proximate users. The architecture contained a central server which stored user profiles with user preferences in a format that was used back in 2004 on social networking sites such as Match.com and LinkedIn.com. Each user profile had to be linked to a unique Bluetooth hardware address (BTIDs) of the corresponding user mobile device. In order to start using the application, a user had to register the BTID (Bluetooth identifier) of their mobile device, link it to their online profile and turn the device into visible mode. When the Serendipity application was running it was able to detect visible proximate mobile devices with the use of BlueWare application designed and implemented by the same research group. BlueWare ran passively in the background of mobile phones and could detect a nearby mobile device, record the information about the newly discovered device in the proximity log and then send the BTID of this device to the central server. Once the central server received the BTID value it could then be able to link it to the corresponding online profile if this user was already registered and calculate the similarity index by extracting and comparing the information about the two users' interests. If the calculated index value was above the pre-defined threshold then the users received anonymous messages notifying that there was a person with similar interests nearby. Both users had to reply with confirmation to these notifications in order to be able to start exchanging the personal information. Finally the users could continue the interaction in real life by, for example, arranging a

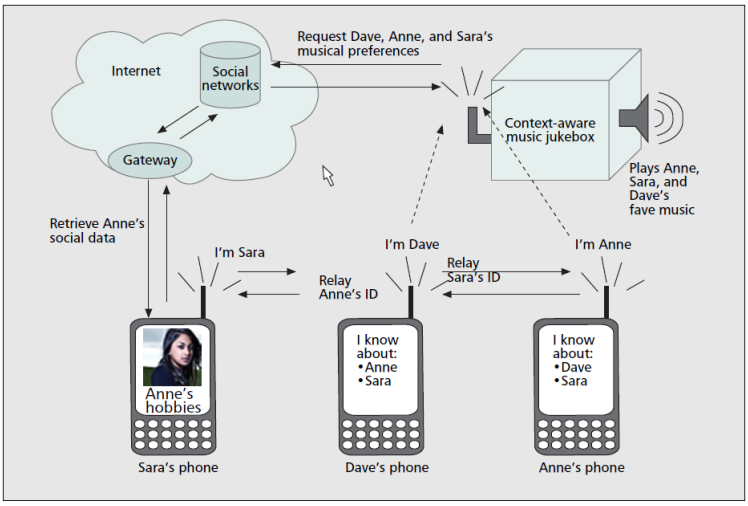


Figure 3.3: The WhozThat infrastructure [BGA+08].

meeting point through the messages. The Serendipity project mainly focused on dating and business purposes. The application was implemented and deployed by a group of students who used the application within the university campus. However since 2005 the project was suspended and no further development was undertaken.

WhozThat project

WhozThat [BGA+08] is a mobile social network proposed by a group of researchers from University of Colorado at Boulder in 2008. The proposed system is similar to Serendipity [EP05] however it is different in a way that users in fact exchange real social networking IDs instead of Bluetooth identifiers by means of direct wireless communication (e.g. Bluetooth or WiFi). After two users exchange the social networking IDs, they are able to lookup the corresponding identity profiles of each other at OSN sites, for example Facebook or LinkedIn. Finally when they receive the information about each other such as interests or music tastes, it is easier for them to meet and communicate in reality. The main idea of WhozThat system is to bring the information from online social networking sites to the local social physical networking, thus enriching the local social interaction between people. Within the project the authors also propose a context-aware service, namely a music player (jukebox) in a bar which is able to adapt the song playlist based on the tastes of people who are in the bar at the moment. The WhozThat system is shown on Figure 3.3. The WhozThat infrastructure supports:

1. Local context/aware services, such as a music jukebox which adapts the playlist based on the tastes of persons through their advertised social IDs though mobile devices,

2. Multihop relaying, and
3. Gateway services which can be used to offload complex, compute-intensive, and memory-intensive operations off from mobile devices to the gateway.

The mobile devices can also support multihop relaying. The mobile devices are supposed to be able to establish the connection to the Internet through cellular telecommunication technology such as EDGE, UMTS, GPRS, HSDPA, 3G or through WiFi/WiMAX.

The exchange of social networking identifiers in WhozThat system is done in clear text [BGA+08], which obviously raises security and privacy issues for the users of this system. Either the users must consent broadcasting their social networking IDs or, which is more favorable, there should exist mechanisms that provide user anonymity. In addition, in order to prevent spoofing attacks some kind of authentication is needed prior contacting the social networks for retrieving the personal information. To enhance the security of WhozThat the authors propose modifications to the design of the system and introduce an intermediate identity server (IS) which is assumed to be a trusted and secure network element. The IS generates Anonymous identifier (AID) for each mobile device which participate in the networking. The AID is a SHA-1 cryptographic value calculated with a 16-byte random salt value. Each AID is associated only with one mobile device, however a device can request multiple AIDs in order to advertise itself to multiple local services at the same time. Prior the participation all mobile device must sign up in order to obtain a user account at IS, the user provides the social networking ID such as Facebook profile id and receives back a username and password to access the IS. The mobile device is then possible to authenticate itself to the IS by means of the username and password securely stored in the mobile device. After the device is authenticated with the IS the IS cab access the users AID, device location, social networking ID. Usually the AID timeout is 30 sec that it prevent from replay attacks. The resources stored at the IS support HTTP methods and each HTTP request is encoded using JSON (RFC 4627 [Cro06]). The communication between the mobile device and IS is done through HTTPS protocol. The access to resources is authenticated using HTTP basic access authentication RFC 2617 [FHBH+99]. The main assumptions of authors is that devices use a secure positioning system, for example SPINE [CH06]. The weak point in this design is the IS, which is the point of failure. The modified design of WhozThat that supports anonymous identifier through the introduction of Identity Server is presented on Figure 3.4.

Popular mobile social networks

The mobile application development is a very active arena. From the mid 2000s onwards mobile devices become ubiquitous and social networking applications are created to be accessed by mobile phones. The developers of mobile applications actively focus on making use of 1) location based services (LBS) which can be accessed with mobile devices and allow to retrieve the geographical location of the

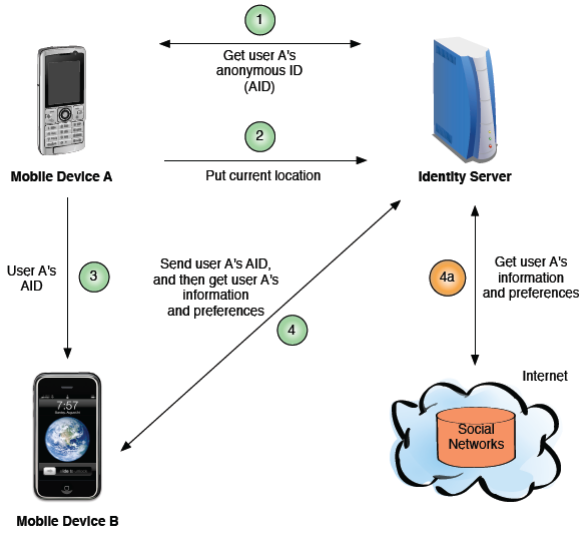


Figure 3.4: The WhozThat system with support for anonymous IDs [BGH09].

device, and 2) Internet access over cellular networks and WiFi networks. Some of the currently popular mobile social networks are Loopt[1], Gowalla[2], Brightkite[3], GyPSii[4], Foursquare[5], Gbanga[6], etc. Interaction with friends in local proximity and invitation of friends to explore new places and venues together becomes a common feature of all these sites.

3.1.5 Extended functionality of mobile social networks

As mentioned before the move of social networking into mobile space signifies the introduction of new means and channels for communication and interaction among users. Mobile social networks hold extended functionality realized by additional mobile technologies, such as location based services (LBS), short message services (SMS), multimedia message services (MMS), etc., and wireless features which include proximity and direct-mode services. On the one hand, with all this technology it is clear that the evolution of mobile social networks has a direction towards more sophisticated ways of communication and interaction between users. On the other hand, it brings new problems to be solved by mobile carriers, mobile manufacturers and service providers. Below is overview of major privacy aspects of location-based services and direct mode wireless communication enabled in the mobile devices.

[1]Loopt, http://www.loopt.com
[2]Gowalla, http://www.gowalla.com
[3]Brightkite, http://www.brightkite.com
[4]GyPSii, http://www.gypsii.com
[5]Foursquare, http://foursquare.com/
[6]Gbanga, http://gbanga.com/

Location-based services

Location-based services (LBSs) are services which are accessed by mobile devices through a cellular network and able to track the position of users and to provide specific information to users based on their locations [VMG+01]. LBSs are widely used in mobile social networks such as Foursquare [Fou11], Gowalla [Gow11] and GyPSii [GyP11]. For example, a user with a mobile device can explore the neighbourhoods or to locate her friends in the close vicinity in order to explore new places together.

Recently much research in the field of LBSs has been carried out with a focus to provide protection of privacy to users. Research efforts mainly improve the underlying system architecture or propose new disclosure-control techniques. Techniques which support location anonymity are proposed in [GG03] and [CM07].

As it is outlined in Section 1.1 the ambition of the SWiN project is to have a mobile social network which functionality covers location based services. Although a vast study was carried out about privacy issues of location based services for mobile social networks, this report does not include it due to the absence of direct relevance with the design modifications described in Chapter 6. The present study deals with design modifications in order to have support for user and group pseudonym within the mobile social network, however it does not deal with pseudonyms in the context of location based services.

Direct wireless communication

Another opportunity for users of mobile social networks is that they can combine traditional web based social networking with direct local wireless communication, e.g. via Bluetooth or WiFi connection. For instance, direct interaction can be used in order to detect existing members in the neighbourhood or to ease the process of membership through introducing new ways of joining a group or community based on physical presence. Functionality of direct wireless communication available on mobile devices significantly extends the usability of social networking. However, with the advent of this combination, the process of establishing security associations should be reconsidered and improved. The document [WF08] presents a key management scheme that combines traditional social networking security association establishment with security association creation via direct local wireless communication enabled in mobile devices. Several security pairing protocols for device authentication are described in Section 3.2.2.

Other technology

It is also possible to track users or provide information services based on RFID technology. In traditional approach to RFID technology readers are considered to be stationary and tags are considered to be mobile (for example, RFID tagged items in a supermarket and gates at the entrance). By integrating RFID technology in mobile telecommunication services tags become stationary and readers (which are

integrated in the mobile devices) become mobile [Sei05]. Service providers can provide information on objects equipped with RFID tags over a telecommunication network [Sei05]. The only main requirement is that a RFID reader must be installed in a mobile device, although it is also possible to introduce applications where a mobile phone can be both a tag and a reader at the same time. Integrating RFID functionality into mobile devices extends the use of RFID technology and introduces RFID-enhanced social networking. The privacy issues and security requirements of RFID technology is discussed in [KSK03], [MW04] and [WSRE03].

Another, recently appeared interesting technology is called Bump[7]. The application enables sharing of information such as personal contacts or media files by means of a simple bumping of two mobile devices. There is no technical specification available for this technology and it is not totally clear how it is implemented. However, the technology requires that the mobile devices have access to the Internet (3G or WiFi) and that location services be turned on. The idea is that when a mobile device bumps another mobile device, the sensors of the first device feel the act of "bumping", prepares the information for the transfer information and sends it to a central matching server. The special matching algorithm at the same time identifies the candidate mobile device that is supposed to receive these data based again on sensors of another device and define the route between two phones. Thus, the geo-location is used to define the device pairs. The second mobile device finally receives the data destined to it from the central matching server over the Internet, not locally via Bluetooth [Bum11].

3.1.6 Legal issues in social networking (EU&US)

The legal framework surrounding Information and Communications Technology is a continuously evolving area of law. The framework is still unsettled but legislation is in motion and a number of directives have already been adopted by the US and EU. The main goal of the directives is to ensure that personal information is not used or disclosed in a way so that it violates personal integrity of individuals. They focus is on defining the types of processing which are allowed and the requirements which should be fulfilled. However the national legislation is always required to give legal effect to the principles of the directives described next.

With the widespread use of social networking legal institutions pay more attention to the new legal issues which constantly arise. These issues include dealing with users' privacy, protection of intellectual property, criminal activities, liability, etc. In the global context the concept of privacy is defined as the ability of an individual to control who has access to their personal information and is considered to be one of the fundamental human rights protected by the legislation [Nat]. Providing users more control over their personal information can help in archiving privacy protection in social networks. However, the social networking sites such as Facebook [Fac11] keep on being criticized for not giving users the absolute right to

[7]Bump Technologies, http://bu.mp/

choose who can view their profiles and access their personal data, thus intensifying the debates around the protection of privacy which is mainly concerned with the appropriate collection and processing of the personal data.

One of the most important European directives in regard to processing of personal information is *Directive 95/46/EC* also known as Data Protection Directive. The document regulates the handling of personal information by organizations in EU countries. It defines a number of concepts and introduces rules and guidelines for processing personal data. The definitions used to describe the legal issues of the processing of personal data follow.

1. According to Article 2 of the directive, *personal data* is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". For example, information such as name, address, telephone number, fingerprints, email address, IP address, etc. are considered to be personal information. In addition, racial or ethnic origin, political opinions, religious or philosophical beliefs, health or sex life, information about friendships, group memberships and other affiliations fall under the category of sensitive information in Article 8.

2. *Processing of personal data* is "any set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction" as it is defined in Article 2.

3. *Data controller* is a body (e.g. a person, public authority, agency, etc.) who "determines the purposes and means of processing".

4. *Data processor* is a body (e.g. a person, public authority, agency, etc.) who is expected to execute and implement the instructions of the controller and processes personal data on behalf of the controller.

Obligations and responsibilities are mainly imposed on the data controller. For example, Article 7 states one of the important criteria for legitimate data processing is that personal data may be processed only if the data subject has explicitly and unambiguously given the prior consent. According to Article 17, the data controller must "implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access". However when it comes to social networking the concept of the data controller is a very complicated and debatable issue. The problem is that not only providers of social networking sites such as Facebook [Fac11]

and Twitter [Twi11], but also third parties and users who post information in these networks are regarded as data controllers. Thus, all three groups together in fact constitute the data controller and must adhere to the legal rules laid down under the directive. Among other issues described in the directive are the rights of the data subject, such as the right of an individual to request the data controller for information about the type and amount of personal data processed about him or her, and rectification and erasure of personal data stipulated in Article 12.

Another important document is *Directive 2002/58/EC* also known as Directive on Privacy and Electronic Communication. The main scope of the directive is the processing of personal data and the protection of privacy in the sector of electronic communications. For example, the directive requires the provision of confidentiality of the communications in Article 5 and the protection against spam in Article 13.

Finally *Directive 2006/24/EC* or Data Retention Directive has a goal to harmonize the regulations regarding the retention of traffic data for the purposes of investigation, detection and prosecution of serious crime. The directive defines the categories of data that should be retained. It also defines that interceptions are allowed only by authorized entities and only in cases which involve certain crime.

The US has no comprehensive legislation in regard to the treatment of data protection or privacy issues. The most important documents are *Privacy Act of 1974*, *Computer Matching and Privacy Act* and *Safe Harbour Principles*. The later document was developed after the introduction of Directive 95/46/EC as a need to meet EU standard requirements. As a matter of fact, Europe and the United States have different approaches to dealing with privacy issues especially in the electronic communication sector. While EU takes a strong regulatory approach, the US is more considerate towards keeping the balance between business demands and data protection. For example, US does not demand from organizations to obtain explicit consent from users before processing personal information as it is required by the European legislation.

As a result, the difference in laws in different countries can act against the harmonization in the field of privacy protection to users of social networks. The conflicts in legislation can have a serious impact on solving crime cases. For example, if an adversary and a victim come from different countries the legislation between which is not harmonized then the court might advocate for the accused one rather than the victim. An interesting fact, is that even though Facebook is founded in the US it must adhere to EU laws in respect to privacy rules as it targets the European audience [ZDN11]. Finally, debates are also held around the issue on who possesses the content of social networks.

The discussion above highlights the need to take into consideration the legal aspects while designing a mobile social network. Protection of personal information of users becomes an increasing concern and one of the pressing legislative plans. As a result, it is advisable to embed legislative compliance within the system during the design phase rather than to introduce necessary changes to meet legal requirements at later stages of the project.

3.1.7 Major privacy threats in mobile social networking

According to [CB95], three levels of privacy can be identified. *Identity privacy* is concerned with hiding the identity of a user. *Location privacy* is concerned with hiding the location of a user. *Content privacy* is concerned with keeping user data safe. Content privacy is related to confidentiality and can be often achieved by means of encryption. It is important to determine which type of user information can be revealed during each procedure supported by the functionality of a mobile social network and how all three levels of privacy can be achieved. The present Master's thesis work addresses and discusses mechanisms for protecting the identity privacy of users, leaving location and content privacy protection outside the scope of this work.

User identity is a unique representation of the information about an individual and may consist of several pieces of information about this individual known as identity attributes or identifiers. Identity management of a system is always a complex and challenging issue to solve. On the one hand, identity attributes can be used to facilitate such procedures as user authentication or access control decisions, but on the other hand, identity attributes often contain sensitive user information and thus need to be protected.

The recent documents of ENISA look closely at security and privacy risks related with identity management [CDFH+11] and particularly mobile identity management [PrB+10] in online communities. The studies propose recommendations how to address the challenges and promote technologies that serve the purpose to protect privacy.

According to the ENISA document [PrB+10] that enumerates major risks and threats to mobile identity management and the study [Kum10] on privacy risks and threats in social networks, a mobile social network is subject to the following major privacy and security threats:

1. **Identity theft:** A form of fraud in which an adversary pretends to be someone else. The cheating is possible if the adversary gets access to personal information, for example, stored on the victim's mobile device. Personal information may include credentials, encryption keys or biometric data. The risk emphasizes the need for secure identification mechanisms to prevent impersonation.

2. **Eavesdropping:** The act of secretly listening to a private conversation without the consent of its participants. In mobile context, transfer of data using Bluetooth technology is especially a subject to attacks by eavesdroppers.

3. **Surveillance and stalking:** An unauthorized monitoring to reveal pieces of personal information. The threat is especially relevant to location based services.

4. **Phishing:** An attempt to acquire pieces of sensitive information by masquerading as a trusted entity.

5. **Profiling:** An attempt to reconstruct a victim's profile based on the obtained pieces of information.

6. **Man in the middle attacks:** An attack in which an adversary operates as a middle entity in connection between a mobile device and some trusted services. Man in the middle attack can be used to monitor user activity or even to perform an identity theft.

7. **Information modification:** An intended change of important information in storage or in transfer.

8. **Redundant information collection:** A collection of additional user private information, e.g. by service providers, which is not necessary to offer a service.

9. **Malware and spyware:** Vulnerable software installed on a mobile device which can collect pieces of information, e.g. address and telephone books.

10. **Inadequate device resources:** A risk caused by the problem that strong algorithms, for example, for authentication or encryption, demand higher processing power and might become a challenge to mobile devices with limited resources.

11. **Threats to protocols**: Potential vulnerabilities and problems of the protocols enabling the mobile social network.

12. **Lack of user awareness:** A challenge related to the need for education users. Users themselves often do not realize to which extent it is normal to share personal information with other users in the network or even with the service provider. The problem also closely deals with challenges to offer user-friendly mechanisms to users, such as privacy mechanisms, to effectively control the amount of information they share in the network.

Specific threats to privacy in a mobile social network can be determined by carrying out a risk analysis.

identity privacy requirements for mobile social networks

The main privacy requirements for mobile social networks that focus on the protection of sensitive identity information of users can be summarized as follows:

1. Users must be registered before they start using the mobile social network.

2. Registration of new users must be carried out in a secure way.

3. Multiple registration of the same physical entity shall not be allowed.

4. The system must check against duplicated personal information upon registration of a new user to prevent profile phishing attacks.

5. Automated registration of users must be detected and blocked.
6. All users must be securely authenticated to the provider.
7. The provider must be securely authenticated to all users.
8. Users must be able to mutually authenticate each other in order to protect themselves against communication with fake or spoofed profiles.
9. All communication channels must be securely cryptographically protected against unauthorized disclosure.
10. Anonymity or unlinkability techniques must be introduced where possible in order to conceal communication relationships.
11. The provider must assure that no confidential information is shared with other parties.

3.2 Identification and key exchange schemes

One of the main challenges to secure communication and interaction in mobile social networks is the problem of strong and secure identification of users in such networks. The consequences, in case of failure, may lead to serious risks for users' identity information. Secure identification and authentication is mainly related to the establishment of security associations for the following communication along the secure channel.

The next section given an overview of protocols enabling the SWiN mobile social network. The SWiN design described in Chapter 4 is based on the 3GPP's standard for secure authentication of users and employs a device pairing protocol for mutual authentication between mobile device during direct mode communication. The GAA standard and an overview of two device pairing protocols, namely MANA and ViDPSec, is described below. The section also provides a description of two security token models for representing user authentication and authorization data, i.e. X.509 certificate standard and SAML assertion format.

3.2.1 Generic Authentication Architecture

The use of social networks on mobile phones, just like other mobile services, requires strong authentication. One approach is that the owners of mobile phones have credentials for each service they access. Often it is simply a combination of a username and password which apart from inconvenience to users, also brings a number of security problems. For example, users may select really weak passwords or reuse the same password to access different services. Of course, it is possible that service providers may take responsibility for managing credentials by providing users with strong passwords with no option to change them manually and regularly distributing new passwords. But this approach is really expensive and infeasible for

the service providers and can be even more difficult and problematic for the users. Another approach is based on the idea of single sign-on. An illustrative example of such approach is the OpenID standard for single sign-on for the Web. The technical specification of the protocol can be found in [Ope]. The goal of the protocol is to provide a decentralized model for authentication of a user to various web sites using only a single identity. A user is free to choose a desired identity provider, however the main assumption is that the identity provider is granted a high level of trust. In addition, authentication process with OpenID is subject to several security issues which are discussed in [DO10], [SKS10], and [OJ08].

GAA stands for Generic Authentication Architecture which is a solution proposed by the 3rd Generation Partnership Project (3GPP) and solves problems of users regarding the management of numerous credentials for different mobile applications and services. GAA provides an increased level of security and serves the purpose of providing mutual authentication between mobile devices such as a mobile or smart phones and services on the Internet or in cellular networks. Since the SWiN project secure identification design described in the next Chapter 4 is an extension of the mobile telecommunication standard GAA the detailed description of the later follows.

The detailed description of the GAA standard can be found in the 3GPP technical specification [3GP07]. A comprehensive overview of GAA standard is also provided by Olkkonen [Olk06] and in the work of Laitinen et al. [LGA+05].

GAA authentication services should be provided by a mobile network operator (MNO) and can be divided into two types of authentication mechanisms:

1. GBA (Generic Bootstrapping Architecture) is based on the secret key shared between the communicating entities [3GP10a].

2. SSC (Support for Subscriber Certificates) is based on digital certificates and public-private key pairs [3GP10b].

The bootstrapping functionality on the mobile or smart phone, which is usually a special bootstrapping client, can be installed either during the manufacturing process or at any time by the user.

Generic Bootstrapping Architecture (GBA)

Details about GBA can be found in the technical specification 3GPP TS 33.220 [3GP10a]. Figure 3.5 shows the entities which are involved in the GBA authentication process and interfaces between them.

UE denotes the user equipment, i.e. the user's mobile device such as mobile or smart phone with has a SIM card. NAF (Network Application Function) is an application server which provides services to users, e.g. mobile TV, and is generally maintained either by a local or external MNO. BSF (Bootstrapping Server Function) is the network element which belongs to the cellular network and is the intermediate node in the communication between a UE and a NAF. HSS (Home

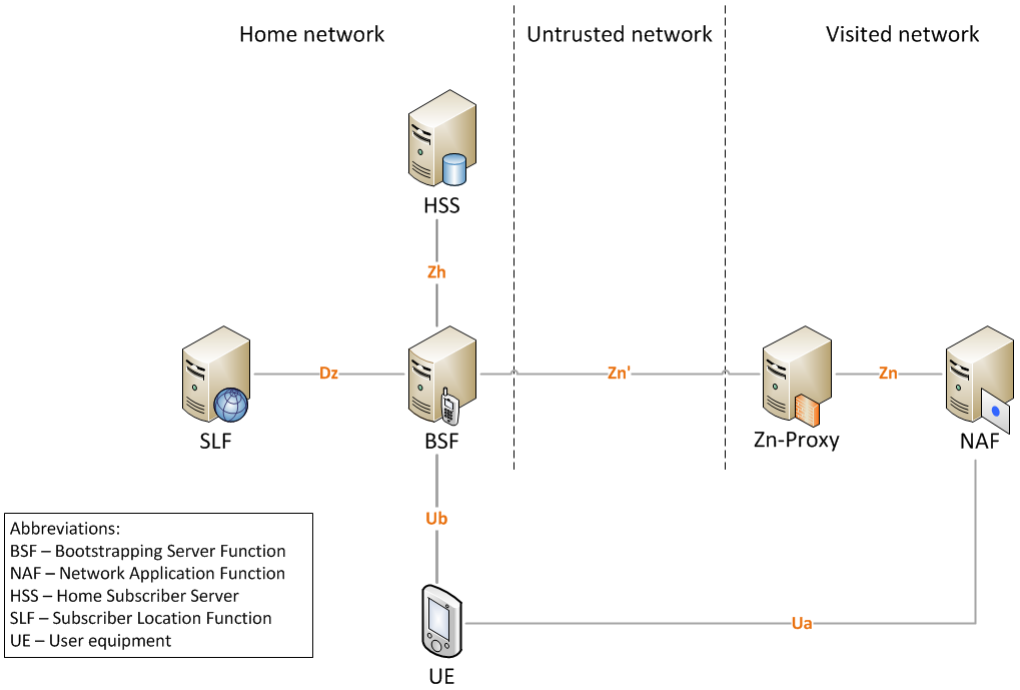


Figure 3.5: Generic Bootstrapping Architecture [3GP10a]

Subscriber Server) resides on the network side. The UE and the HSS share a secret which is never transferred over the network. The secret is stored in the SIM card of the UE on the client side and by the HSS on the network side. When a user would like to access a service, the UE first contacts the NAF over the interface Ua. The Ua interface is application independent and can be any protocol used by the application. If the NAF requires GBA it responds back to the UE with the bootstrapping initiation request. When the UE gets the response it performs a bootstrapping authentication to the BSF maintained by the MNO along the Ub interface. The Ub interface provides mutual authentication between the UE and the BSF based on the 3GPP AKA infrastructure [3GP08] and HTTP Digest AKA protocol [NAT02]. The Ub interface thus represents the bootstrapping authentication procedure. The BSF retrieves data about mobile subscribers from a HSS (Home Subscriber Server) or HLR (Home Location Register) over the Zh interface using Diameter Base Protocol. If there are several HSSs maintained by the MNO then the BSF needs to communicate first with the SLF (Subscriber Location Function) over the Dz interface in order to find out which HSS to use. The Dz interface is considered being optional and its usage depends on the concrete MNO. The BSF communicates with the NAF along the Zn interface during the bootstrapping usage procedure. If the NAF is located in the mobile network different from the home network then it uses Zn-proxy in order to communicate with the BSF.

There are two variants of using GBA and they depend on the SIM card capa-

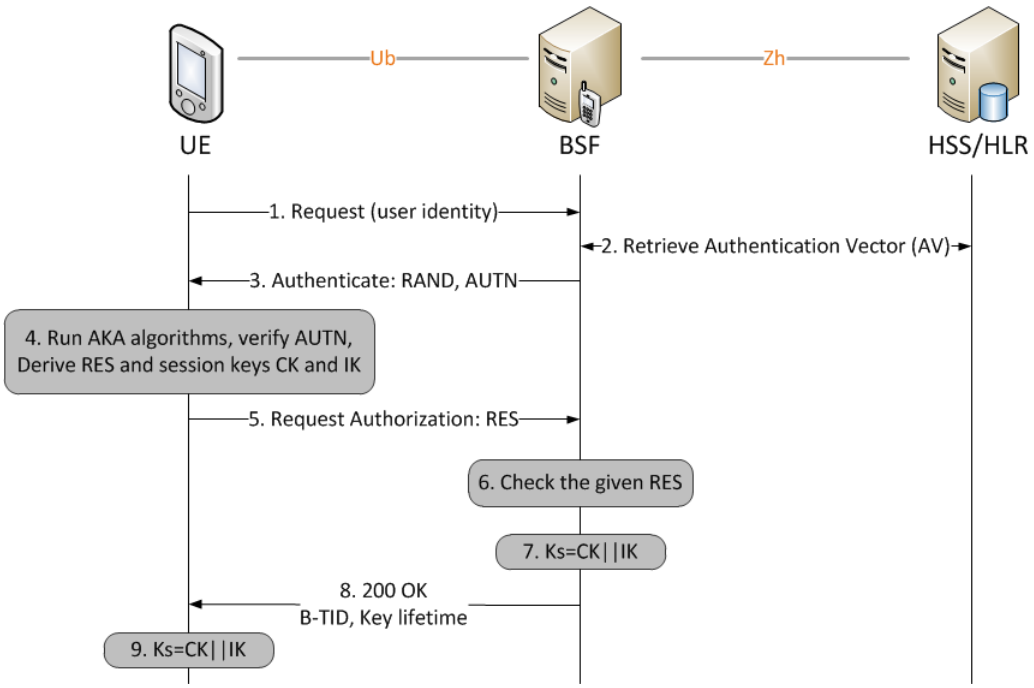


Figure 3.6: The bootstrapping authentication procedure [3GP10a]

bilities. *GBA_ME* is defined as the "default" GBA scheme. Since by default the UICC is GBA-unaware, GBA stores the keys outside the SIM card and uses the ordinary AKA authentication scheme. *GBA_U* is GBA but with UICC-based enhancements. It stores the keys on the UICC (Universal Integrated Circuit Card) and the SIM card calculates session keys. GBA_U is a more secure scheme but it requires additional modifications to UICC.

The HSS stores the set of all users' profiles known as *GBA User Security Settings* or GUSS. Each user profile or USS is an application and subscriber specific parameter set and consists of two parts. The authentication part includes a list of identities of the user needed for the application. It can be IMSI (International Mobile Subscriber Identity), IMPU (IP Multimedia Public Identity), MSISDN (Mobile Subscriber Integrated Services Digital Network Number), pseudonym, etc. The authorization part which includes details about various user permissions , e.g. if this user is allowed to access this particular application. The USS can also mention the type of GBA that can be carried out, such whether the device supports GBA_U or GBA_ME [3GP10a]. The BSF can obtain USS of a user from the HSS over the interface Zh. The NAF can obtain the USS from the BSF upon a request from the NAF during the bootstrapping usage procedure over the interface Zn.

The message flow of the bootstrapping authentication procedure is shown on Figure 3.6 and the detailed steps are given below:

1. The UE sends a request with the user identity (username) to the BSF.

2. The BSF sends a request to the determined HLR/HSS over the Zh or Zh' interface with the username and required profile items. The later means that the BSF can request only some of the user profile information elements, but in most cases the BSF would ask for the full user profile. The HLR/HSS sends back to the BSF the retrieved elements of the user profile (GUSS) together with the Authentication Vector (AV). 3GPP Authentication Vector (AV) contains a random number (RAND), authentication token (AUTN), expected response (XRES), cipher key (CK) and integrity key (IK) values, i.e. $AV = RAND||AUTN||XRES||CK||IK$.

3. The BSF forwards RAND and AUTN values to the UE.

4. The UE checks AUTN to authorize the network and runs the AKA algorithms to calculate the RES value and the session keys CK and IK.

5. The UE sends to the BSF the second request containing the derived RES value in order to get authenticated by the network.

6. The BSF authenticates the user by comparing the RES value received from the UE with the XRES value stored in the authentication vector. If these values match then the UE is authenticated and the BSF calculates a B-TID (Bootstrapping Transaction Identifier) from the RAND value and the BSF server name.

7. The BSF derives Ks key by concatenating the CK and IK keys.

8. The BSF sends to the UE the 200 OK response message which contains the calculated value of B-TID together with the lifetime of the Ks key.

9. The UE derives Ks key through the same procedure of concatenating the CK and IK keys.

The Bootstrapping Transaction Identifier (B-TID) serves the purpose to bind the subscriber identity to the key material Ks over the interface Ua. B-TID is considered to be globally unique and a NAF should be able to identify the home network and the BSF of the UE based on the provided B-TID. The B-TID value is generated by taking the base64 encoded RAND value which is a field in the Authentication Vector (AV) supplied by the HSS and the BSF server name. However although B-TID functions as an anonymous identifier of a user, the use of B-TID does not provide the "service continuity" because each time a user updates the key it contacts the NAF with a new B-TID value and the NAF is not able to determine whether it is the same user.

The session secret key Ks established during the bootstrapping authentication procedure between the UE and the BSF is used later on for the secure communication between the UE and the application server (service provider). Both the UE and BSF store the calculated key value Ks. The UE also stores the RAND value. However, in fact, the Ks is not used directly as the session key for the communication

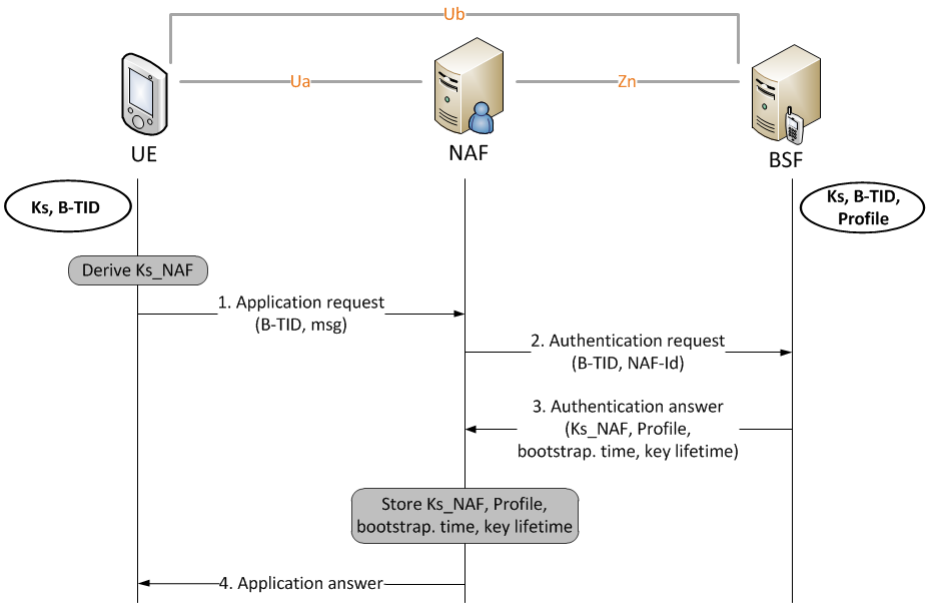


Figure 3.7: The bootstrapping usage procedure [3GP10a]

between the UE and the NAF but only as the key material to produce the actual session key Ks_NAF. Ks_NAF is computed from the Ks during the bootstrapping usage procedure when the UE contacts the NAF.

The message flow of the bootstrapping usage procedure is shown on Figure 3.7 and the detailed steps are given below:

1. Before the UE contacts the NAF, it derives the actual session key Ks_NAF from the stored key material Ks. The Ks_NAF is created with a special key derivation function that uses as parameters the IMPI of the UE, the NAF-ID and RAND values among others. The UE starts the communication with the NAF over the interface Ua. The UE sends an application request with the B-TID value to the NAF. The message can also contain the application specific dataset which is not of the interest in the present context.

2. The NAF forwards the authentication request to the BSF over the interface Zn in order to get the session key corresponding to the given B-TID. The NAF also includes the NAF-ID value which is the NAF's public hostname used by the UE in the authentication request.

3. The BSF authenticates the NAF and verifies that the NAF is authorized to use the given hostname. If the verification is successful then the BSF derives the Ks_NAF key from the Ks key material which corresponds to the given B-TID using the same key derivation function. The BSF sends back to the NAF the session key Ks_NAF with its bootstrapping time and its lifetime. In addition to Ks_NAF, the NAF can also request some application specific information

elements from the user profile from the BSF such as the user identity which can be the user's IMPI, MSISDN, IMSI or the user's pseudonym. If no identity is transferred to the NAF then the user remains anonymous towards the NAF and the B-TID functions as the temporary user identifier. However the use of B-TID does not provide the "service continuity" because each time the user updates the key it would contacts the NAF with a new B-TID value and the NAF would not be able to determine whether it is the same user.
If no session key is found for the given B-TID, then the BSF reports it to the NAF which in turn sends a bootstrapping renegotiation request to the UE. In this case the UE must perform the bootstrapping authentication procedure again as described above.

4. The NAF stores the session key Ks_NAF, its bootstrapping time and the lifetime. The NAF sends application answer to the UE.

In the case of bootstrapping with UICC-based enhancement (GBA_U), the keys CK and IK never leave the UICC. When the UE receives the challenge from a BSF, the mobile equipment (ME) sends RAND and AUTN values to the UICC which in turn calculates CK, IK and RES values. It also checks AUTN in order to verify that the challenge is received from the authorized network. Then the UICC transfers RES value to the ME and stores Ks. The ME sends the challenge response to the BSF based on the calculated by the UICC RES value and thus becomes authenticated by the BSF. Now both the BSF and UICC are able to create NAF-specific keys Ks_ext_NAF and Ks_int_NAF. The former key the same as in the GBA_ME case. And the later key is calculated with slightly different parameters as input for the derivation function. It should be noted that during the bootstrapping usage procedure the UE and the NAF must also agree which type of keys to use, Ks_ext_NAF, Ks_int_NAF or both. The default key is always Ks_ext_NAF, because it is supported by UEs which are not GBA_U compatible. The NAF must also always notify the BSF if it supports GBA_U or not.

Support for Subscriber Certificates (SSC)

Support for Subscriber Certificates (SSC) is described in detail in the 3GPP technical specification 33.221 [3GP10b]. The main idea of the certificate support for GAA is to provide registration of users' public keys and corresponding client certificates.

In the SSC architecture the GBA network element NAF is replaced with a PKI Portal (see Figure 3.5). Authentication of a UE to the PKI Portal is done with the use of GBA mechanism described in Section 3.2.1. The task of a PKI Portal is to issue subscriber certificates for UE and to deliver operator CA certificates. The GAA PKI Portal can be either a Registration Authority (RA) who authenticates the certification requests based on the cellular subscription or it can also combine the functions of a Certification Authority (CA) that issues certificates. In case when a PKI infrastructure already exists in the network the PKI Portal functions only as a RA and the CA is located within the PKI infrastructure. The BSF supports

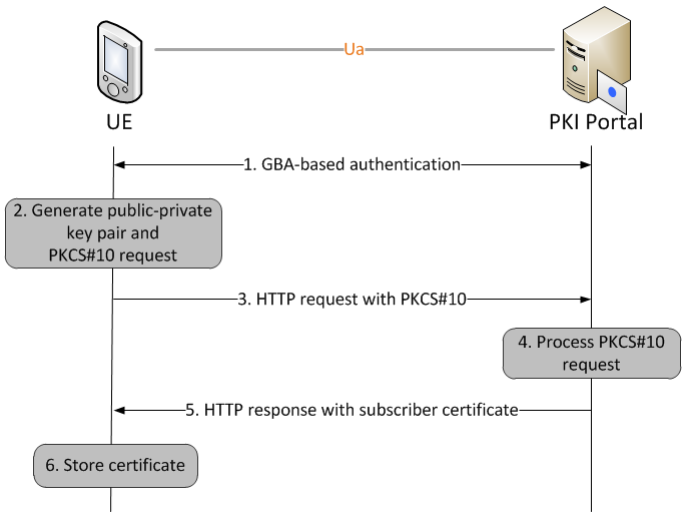


Figure 3.8: The procedure of issuing a subscriber certificate [3GP10b]

the PKI portal by providing authentication and PKI Portal specific user security settings, e.g. the types of certificates UE is allowed to enrol. The communication between a UE and the PKI Portal is protected with the secret session key established between the UE and the BSF during the bootstrapping authentication procedure as it is described above.

A subscriber certificate is issued to a mobile subscriber upon the request from a UE. The supported format of the certificate request is PKCS#10. Upon receiving the PKCS#10 certificate request from the user, the PKI Portal certifies the public key according to its own certification policy and subscriber's user security settings which are fetched through the BSF from the HSS. A subscriber certificate includes the subscriber's public key and other information such as the user identity. Subscriber certificates are signed by the CA with its private key. The UE can also decide to request the PKI Portal for the CA's certificate. A CA certificate identifies the Certification Authority, includes the public key of the CA and is self-signed by the CA.

The key generation procedure should take place on the client side. To ensure that the private key never leaves the UE, the UE might have a WAP Identity Module (WIM). WIM is used to store the private key and is characterized as a tamper resistant device which is capable of providing a proof of that the key is actually securely stored in it. WIM can either be a separate hardware module or a software component on an existing SIM card.

Figure 3.8 shows the message flow of the procedure for issuing a subscriber certificate. The UE is first authenticated to the PKI Portal according to the GBA bootstrapping usage scheme described above. When authentication is complete the UE generates a public-private key pair and a PKCS#10 request for certificate. The UE sends the HTTP request with PKCS#10. If the PKI portal is not a CA it

forwards the request to a one in the existing PKI infrastructure. After the request has been processed the new certificate is delivered to the PKI portal. The PKI portal sends a response to the UE which includes either the certificate itself or a pointer to one (URL) or a full certificate chain.

3.2.2 Secure pairing protocols for mutual device authentication

According to the SWiN design described in Chapter 4, users' mobile devices should perform mutual authentication and establish a security association prior performing an offline invitation through direct mode communication. The establishment of security associations between devices is important for the subsequent secure communication between these devices. Setting up security associations between wireless devices without the need for a trusted third party is called *device pairing*. The idea behind secure pairing is to carry out an authenticated key agreement for the establishment of a session key for the following exchange of data over a secure channel. Several different algorithms and schemes have been proposed to solve the problem of secure device pairing. These protocols often use as visual or aural channel for human verifiable authentication methods as out-of-band control channel. The protocols are also often supported by manual operations such as copying the output data from one device as an input to another device or entering the same data on both devices. The description of two notable protocols for manual authentication of mobile devices [GMN04] and [ZKT] are given next.

Manual authentication for wireless devices (MANA)

MANA is a family of three authentication protocols used for mutual authentication of mobile devices. The protocol version depends on device characteristics and user input. The three protocols are [GMN04]:

1. *MANA I scheme* is used where one device has a display and another device has a keypad.

2. *MANA II scheme* is used where both devices have displays, but none of them has a keypad.

3. *MANA III scheme* is used where both devices have keypads and is based on MAC (Message Authentication Code).

In the context of mobile social networking users interact by using their mobile devices such as mobile or smart phones. These devices typically have both a display and a keypad. The detailed steps of MANA III schemes are shown on Figure 3.9.

Suppose two users would like to perform the mutual authentication in order to verify the integrity of previously obtained data D (e.g. a session key). First of all, both users generate a random string R and enter it in both devices. When the protocol is started device A generates a random value K_A and device B generates a random value K_B. The devices then calculate corresponding MAC values M_A

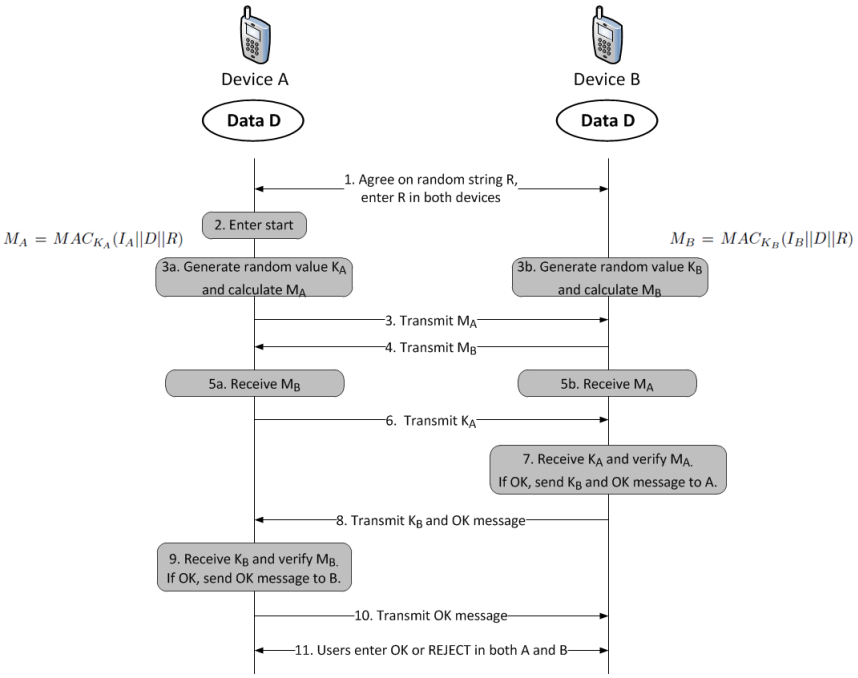


Figure 3.9: The MANA III authentication scheme [GMN04]

and M_B. The calculation is done by using the corresponding K_A and K_B as MAC keys and the concatenation of the device identifiers, data string D and R as an input, i.e. $M_A = MAC_{K_A}(I_A||D||R)$ and $M_B = MAC_{K_B}(I_B||D||R)$. The devices exchange the calculated values of MAC. After device A receives MAC value M_B from device B it sends its MAC key value K_A to the device B. When B receives K_A from A it recomputes the MAC value, compares to the previously received MAC value M_A from A and if they match it notifies A that the verification is successful. If verification is accepted then B in turn sends its MAC key K_B to A. When A receives K_B from B it recomputes MAC value and compares with previously received MAC value M_B from B. If they match then A notifies B that the verification is successful. After both users verify MAC values and in case both verifications are successful then the users can manually approve the authentication by entering for example OK. In this scheme the value of R never leaves the device, thus making it hard for an attacker to intercept the authentication.

Visual device pairing security protocol (ViDPSec)

ViDPSec protocol is based on MANA III scheme in the sense that it also uses verification by a human user as an out-of-band channel [ZKT]. The main difference is the proposal of an additional concept of Device Session Signature (DSS) as a security fingerprint of the device, new for every session. The requirement posed on mobile devices that participate in the authentication scheme is that they both must

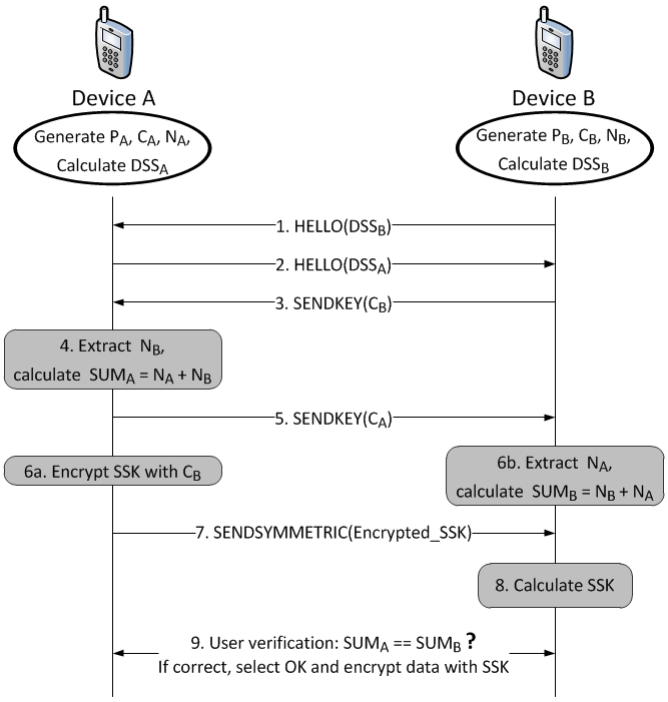


Figure 3.10: The ViDPSec scheme [ZKT]

have displays.

The detailed steps of the protocol are shown on Figure 3.10. The protocol starts with the phase of initiation during which each device generates an asymmetric key pair (P private key and C public key), using any algorithm, e.g. Diffie-Hellman, DSA or elliptic curve. A random number N is also generated on each device and is encrypted with the private key P resulting in DSS fingerprint for the current session. Then devices exchange corresponding DSS values and public keys C. Next, device A sends the session key SSK encrypted with the public key C_B of device B where SSK is calculated with any algorithm, e.g. blowfish, 3DES, IDEA. Device B, in turn, decrypts the SSK using its private key P_B and extracts the session key SSK. The verification is done by comparing the values of numbers which are sums of two random numbers generated on each device in the beginning. In case of a successful verification these numbers must be equal. Now users can continue secure communication by using the exchanged session key SSK.

3.2.3 Security token models

Being a member of a social network implies that a user holds various tokens carrying security information such as authentication or authorization data. This section introduces X.509 standard for public key certificates and SAML standard for transferring authentication and authorization data in a format of assertions which are

used in the SWiN design described in Chapter 4.

X.509 certificates

A complete description of the X.509 standard can be found at [CSF+08]. Certificates serve the purpose to bind the user's identity (or pseudonym) to the corresponding public key and are signed by a trusted Certification Authority. X.509 v3 certificate standard allows to include optional extensions which can be used to extend functionality and thus is the most prevalent type of digital certificates. According to X.509v3 standard, a certificate includes parameter fields as follows [CSF+08]:

- Certificate
  - Version
  - Serial Number
  - Algorithm ID
  - Issuer
  - Validity
    - Not Before
    - Not After
  - Subject
  - Subject Public Key Info
    - Public Key Algorithm
    - Subject Public Key
  - Issuer Unique Identifier (optional)
  - Subject Unique Identifier (optional)
  - Extensions (optional)
  - ...
- Certificate Signature Algorithm
- Certificate Signature

Traceable pseudonymous certificates

RFC 5636 "Traceable Anonymous Certificates" [PPW+09] describes a model and protocol for certificate issuance providing both privacy for users who request and use X.509 certificates containing pseudonyms and an ability to map an anonymous certificate to the individual to whom it was issued under special circumstances thus ensuring traceability of certificates.

The main idea is that the architecture should include two separate authorities involved in issuing certificates. One authority named *Blind Issuer* (BI) should be

responsible for verifying the ownership of a private key. The BI usually acts as a Registration Authority (RA). The second authority called *Anonymity Issuer* (AI) should be responsible for validating the contents of the certificate. The functions of the AI are common to the functions of a Certification Authority (CA). In other words, the main requirement of the approach is a strong separation between the RA and CA roles. The RA and CA should collaborate to reveal a user's real identity only under special circumstances. The split responsibility of two authorities is archived through the technical means of threshold cryptography for digital signature scheme and blind signing technique. The threshold signature scheme means that the RA and CA share a private key for signing and need to cooperate to sign a certificate. The blind signature technique is used to ensure that the content of a certificate being signed is not made visible to the signer and is archived through the cryptographic means.

Figure 3.11 illustrates the certificate issuance procedure steps defined in [PPW$^+$09]. The brief description of the issuance process is given below.

1. The user authenticates himself to the RA. It should be noticed that the in the proposed model a user is assumed already registered with the RA. The RA has a record in the database for each user which contains a user profile information and a corresponding unique identifier called UserKey used as a key to retrieve the information about the user.

2. The RA sends to the user a special data structure called token. The token consists of the UserKey and the TimeOut value, and is digitally signed by the RA. Upon receipt the user verifies the signature of the token and based on the TimeOut value ensures that the certificate request is completed before the token is expired.

3. The user prepares a certificate request in any standard format, e.g. PKCS#10. The user generates a pseudonym and uses it as the Subject field in the certificate request. The user sends the certificate request together with the token as an attribute in it to the CA.

4. Upon receipt the CA performs standard for a CA checks. It verifies the format of the certificate request, performs a private-key proof-of-possession check [HP00] and verifies the uniqueness of the chosen pseudonym. It also verifies that the request contains a valid token. Next, it constructs a certificate and assigns a serial number to it. Then the CA computes a hash over the certificate and blinds the hash value. Blinding process is the encryption of the hash value using a key from a public-private encryption key pair where none of the keys ever leave the CA. Although, the document does not mention any specific algorithm for blinding, one possible scheme is RSA blinding [Lab]. To illustrate, if h is the certificate hash, (N, e) and (N, d) are undisclosed public and private keys respectively, and r is a random value, relatively prime to N, then the hash value is blinded by the random value r as follows $hr^e \ mod \ N$.

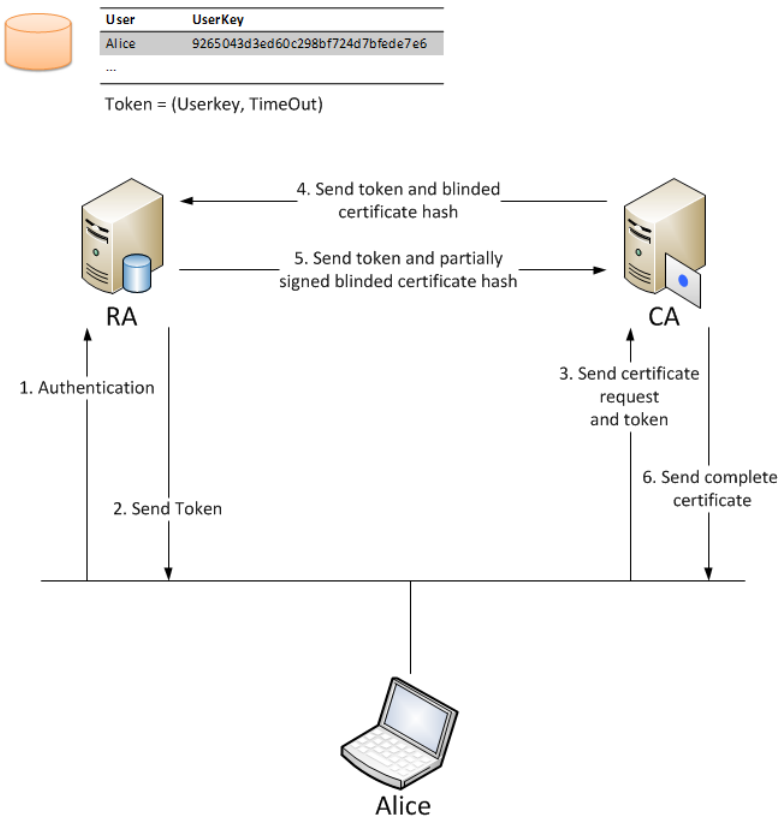


Figure 3.11: The issuance procedure of traceable anonymous certificates [PPW+09]

After the certificate hash is blinded the CA signs the blinded certificate and sends to the RA together with the token.

5. The RA receives the blinded certificate hash and the token and first of all verifies the signatures on the blinded certificate hash and on the token. The RA also checks that no certificate was issued for this token previously. The RA partially signs the blinded certificate hash using its share of the threshold private key and sends back the signed data to the CA.

6. The CA again verifies the signature of the token and partially signed blinded certificate hash. It compares the token against the list of outstanding requests to the RA. Then the CA unblinds the certificate hash by inversing the encryption by using another key from the public-private encryption key pair used for blinding in Step 4. The CA retrieves the partially signed certificate hash. Next, it uses its share of the private key to complete the signature of the certificate and sends the ready certificate to the user. The CA also stores the new certificate and the corresponding token in its database.

RFC 5636 defines an experimental protocol which means that it is not specified as any standard (as of June 2011). The same scheme in fact can be used for any format of data structure, be it X.509v3 certificate [CSF+08] or SAML assertions [CKPM05]. The applicability of RFC 5636 in the SWiN architecture is discussed later in Section 6.2.3.

SAML assertions

Security Assertion Markup Language (SAML) is an XML-based standard [CKPM05] which defines a format for transferring identity information between different domains. A SAML assertion is a structure which contains a series of statements about a subject. Assertions can contain the following statements: authentication statements, attribute statements, authorization decision statements, etc. SAML also allows to encrypt the subject, attributes, or the whole assertion. This can be used to protect the privacy of the users [CKPM05].

Chapter 4

Initial SWiN project secure identification design

The chapter gives an overview of the initially proposed design carried out in the SWiN project [SIC] with a particular focus on identification, authentication and invitation techniques.

4.1 Protocol overview

The model of identification and key exchange scheme for a mobile social network is proposed within the SWiN project [SIC] and its implementation in a prototype is discussed in [Naw11]. The main goal of the design is to guarantee that identification and key exchange processes are carried out in a secure way. The protocol is based on the integration and extension of existing standards to support communication of users of a mobile social network in both online and offline modes. The combination of online social networking with direct mode communication extends the usability of a mobile social network.

- In *online mode* the user interaction is carried out via the new network element called Mobile Social Network Portal (MSNP) and supported by the existing network infrastructure. For example, users can register and authenticate themselves to the mobile social network as well as to perform several online mode procedures such as mutual online authentication of other registered users or online invitation of registered users to join a particular closed group.
- In *offline mode*, instead, communication between user devices and the MSNP is assumed to be temporarily lost or unavailable, however the interaction between registered users can still be carried out through the direct local wireless communication, e.g. via Bluetooth or WiFi connection. To exemplify, registered users can still perform some functionality such as offline user enrolment to a particular closed group.

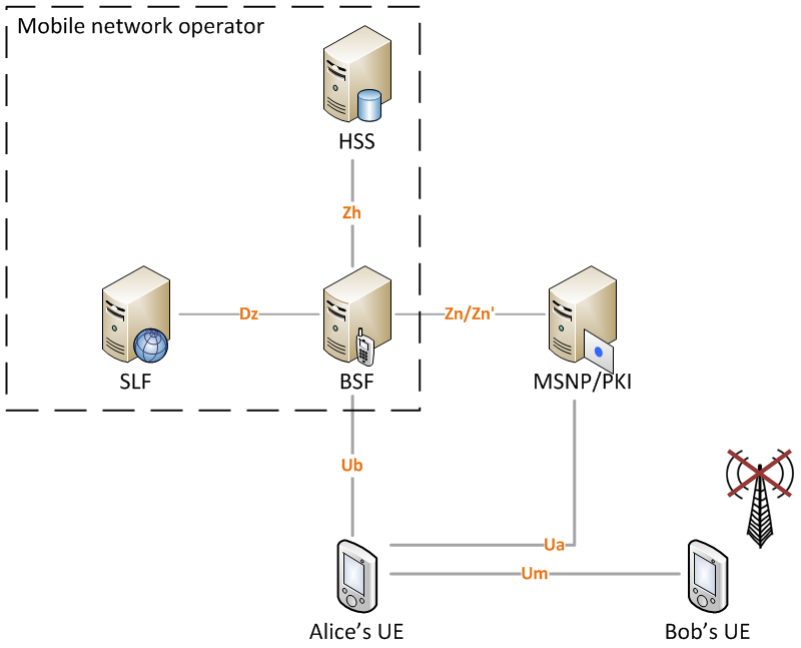


Figure 4.1: Identification and key exchange scheme for a mobile social network [Naw11].

Figure 4.1 illustrates the network elements and interfaces involved in the protocol design. The protocol is an extension of the Generic Authentication Architecture (GAA) telecommunication standard briefly covered in Section 3.2.1 to support the Mobile Social Network Portal (MSNP). Generic Bootstrapping Authentication (GBA) [3GP10a] is used for bootstrapping authentication to generate subsequent session keys for communication between a UE and the MSNP. Support for Subscriber Certificates (SCC) [3GP10b] is used for certification procedures.

4.2 Network elements

MSNP

A Mobile Social Network Portal (MSNP) is a network element which a user's mobile device, or user equipment (UE), communicates with. The MSNP provides such facilities to users as new user registration, authentication of registered users, mutual authentication between registered users, new group creation, invitation of registered users to groups, etc. The details of these procedures are given in Section 4.4. The MSNP also stores a database that contains both user credentials and social information about users such as user profiles, user groups, pending group invitations, user roles within groups, etc. Thus, the MSNP is responsible for secure identity and group handling.

The MNSP also acts as a Certification Authority (CA) and must meet the requirements mentioned in [3GP10b]. As a CA it creates, updates and revokes certificates for users of the mobile social network. It completes a user authentication through a bootstrapping procedure by obtaining the corresponding key to protect the protocol used over the interface Ua and other application specific information elements as a part of User Security Settings (USS) over the interface Zn from the BSF (see the bootstrapping usage procedure, Section 3.2.1).

BSF, HSS and SLF

The networks elements BSF, HSS and SLF are managed by a MNO and their roles are described in details in Section 3.2.1. These network elements of the protocol design are standardized by 3GPP and thus are assumed being trusted.

UE

Following the proposed description a UE meets all the requirements for the GAA mentioned in [3GP10a] and [3GP10b]. To interact with the MSNP over the interface Ua, i.e. for managing certificate enrolments and signing procedures, a special plug-in for web browser or a special client application must be installed on the UE. To be able to communicate with the MSNP over the Ua interface a UE must also have a support for SSLv3/TLS protocol specified in RFC 4366 [BWNH+06].

4.3 Interfaces

Zn, Zh, Dz interfaces

The interfaces Zn, Zh, and Dz are standardized according to the GAA standard and specified in [3GP10a]. The protocol design under discussion does not introduce any changes to these interfaces.

Ub interface

The Ub interface represents a communication channel between a UE and the BSF for negotiating on session keys for the subsequent interaction between the UE and the MSNP. The interface represents the bootstrapping authentication procedure based the pre-shared key stored on the SIM card inside the UE on the client side and by the HSS on the network side. The authentication mechanism is based on 3G AKA protocol.

Ua interface

The Ua interface represents a security association between a UE and the MSNP based on the session key negotiated during the bootstrapping authentication procedure along the Ub interface. The interface represents a communication between

a user and the MSNP and also embodies the processes of obtaining user and CA certificates. According to the 3GPP standard [3GP10a], the Ua interface is application-independent and can be chosen to be any protocol. In the present design the communication channel Ua is established with the use of SSLv3/TLS protocol [BWNH+06].

Um interface

The Um interface represents a communication channel between two mobile devices which interact in offline mode when at least one of them is not connected to the MSNP. The communication can be carried out either over Bluetooth or WiFi connection. A device pairing protocol for mutual authentication should take place prior the transfer of information such as an invitation to a particular group. One possibility is to use one of the device pairing protocols for mutual authentication previously described in Section 3.2.2, e.g. MANA or ViDPSec.

The security and privacy aspects of GAA standard, wireless communication technology (Bluetooth, WiFi) and device pairing protocols for mutual authentication are not considered in the present work and are assumed being correctly implemented in a prototype of the proposed design.

In the following sections a detailed description of registration, authentication and invitation procedures is given with a particular focus on the format of exchanged information and protection of this information in transfer and in storage. An important assumption to mention is that the MSNP and the network operator have the necessary agreements for using GBA.

4.4 Functionality

The current design supports the following functionality for users:

1. New user registration.
2. Authentication of registered users.
3. New group creation by a registered user.
4. Group invitation by the moderator of the group in online and offline modes.
5. Mutual authentication between members of the same social group .

4.4.1 User registration

The steps involved in the procedure of secure registration of a new user in the MSNP are illustrated on Figure 4.2. The user is assumed to have a pre-installed client application.

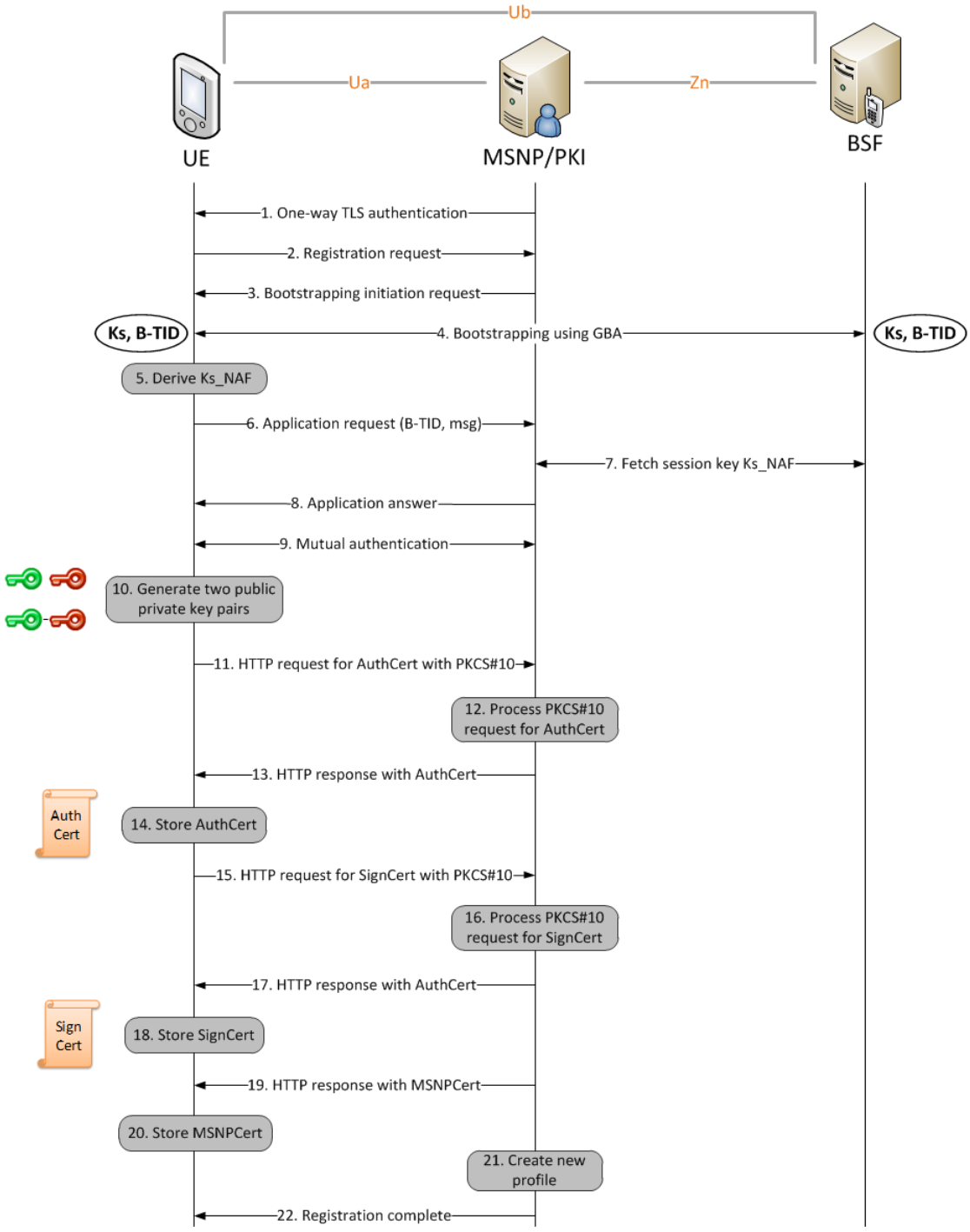


Figure 4.2: The initial SWiN design: User registration.

1. A new user accesses the MSNP through a web browser with a special plug-in or through a special client application installed on the UE. Before the actual registration process starts, a one-way TLS authentication takes place during which the MSNP presents its server certificate to the user. The one-way TLS authentication prior the registration process itself is established to prevent an adversary from listening to the registration communication.

2. When the secure connection is established, the user issues and sends a registration request. The registration request message does not include any GBA-related parameters because at this point the UE is not aware whether the further communication between the UE and the MSNP is carried out based on the GBA standard. The registration request however contains a request for further communication instructions.

3. The MSNP verifies the identity of the user by checking if the user with the provided MSISDN has not already been registered. Since the subsequent communication between the UE and the MNSP over the Ua interface is based on shared session keys obtained during a bootstrapping authentication procedure, the MNSP replies with a bootstrapping initiation request message.

4. The UE and the BSF perform bootstrapping authentication procedure over the Ub interface as specified in [3GP10a] and is previously described in Section 3.2.1. As a result of the successful bootstrapping procedure, both the UE and the BSF derive the key material Ks and the Bootstrapping Transaction Identifier (B-TID) which correspond to the MSNP.

5. After the bootstrapping is completed the UE and the MNSP need to establish the shared key required to protect the Ua interface. To do so the UE derives the session key Ks_NAF from the key material Ks which corresponds to the MSNP application as specified in [3GP10a].

6. The UE sends an application request to the MSNP which contains the corresponding B-TID. The format of the message is specified in [3GP10a].

7. The MSNP fetches the corresponding Ks_NAF from the BSF over the Zn interface based on the presented NAF-ID that belongs to the MSNP and the B-TID provided by the UE in the previous step. The BSF derives the session key from the stored key material Ks according to the derivation parameters submitted by the MSNP.

8. When the key derivation is completed, the MSNP obtains the Ks_NAF from the BSF and stores it along with the bootstrapping time and the lifetime parameter of the key. The MSNP now holds a secure communication with the UE over the Ua interface. The MSNP replies to the UE with an application answer which also contains additional parameters for the following PKCS#10 request generation. If the key derivation cannot be performed, e.g. due to an

expired lifetime of the key material Ks, the MSNP replies to the UE with a bootstrapping renegotiation request to the UE, and the algorithm rolls back to step 4.

9. To proceed with the registration the parties perform mutual authentication based on challenge/response in order to determine that they share the same key Ks_NAF. After that the UE and the MSNP can proceed with the communication over the interface Ua in a secure way.

10. The UE automatically generates two public-private key pairs, and prepares two certificate requests (CSR) in a PKCS#10 format: one for a user *authentication certificate*, and one for a *signing certificate*. The private keys never leave the user device and are stored securely. In the original protocol design the structure of user authentication and signing certificates follows the X.509 v3 certificate standard which supports optional extensions as specified in RFC 5280 [CSF+08] and allows flexibility in a way that extension fields can include some information needed for the MSNP.

    At this step the user is required to provide the following information to complete the Subject field since Subject field binds a certificate to a particular user:

    - Country Name (2 letter code, e.g. SE)
    - State or Province Name (full name, e.g. Stockholm)
    - Locality Name (city, e.g. Kista)
    - Organization Name (e.g. KTH)
    - Organizational Unit Name (e.g. ICT)
    - Common Name (e.g. your name or your server's hostname)
    - Email Address (e.g. elena@kth.se)

11. The UE submits the PKCS#10 request for authentication certificate to the MSNP using HTTP Digest request as discussed in Section 3.2.1.

12. The MSNP processes the PKCS#10 request. Being a Registration Authority the MSNP creates a new authentication certificate for the user and as a Certification Authority the MSNP digitally signs it. The certificate enrolment is carried out in accordance with the certificate enrolment procedure described in [3GP10b].

13. The MSNP sends the authentication certificate as an HTTP response as described in Section 3.2.1.

14. The UE receives the authentication certificate and stores locally on the mobile device.

15. The UE submits the PKCS#10 request for signing certificate to the MSNP using HTTP Digest request as described in Section 3.2.1.

16. The MSNP processes the PKCS#10 request. Being a Registration Authority the MSNP creates a new signing certificate for the user and as a Certification Authority the MSNP digitally signs it. The certificate enrolment is carried out in accordance with the certificate enrolment procedure described in [3GP10b].

17. The MSNP sends the signing certificate as an HTTP response as described in Section 3.2.1.

18. The UE receives the signing certificate and stores locally on the mobile device.

19. The MSNP also sends to the UE a certificate that contains the public key of the MSNP (CA) certificate.

20. The UE receives the signing certificate of the MSNP (CA) and stores locally on the mobile device.

21. The user optionally provides other social information to complete the user profile.

22. The MSNP responds with a message that states that the registration is complete.

The steps 11-14, 15-18 and 19-20 can be done in parallel. The UE receives different certificates of the MSNP in the steps 1 and 19 - the first certificate (received in step 1) serves the purpose to authenticate the MSNP during the TLS handshake, while the second certificate (received in step 19) is used to verify the certificates signed by the MSNP.

4.4.2 User authentication

The steps involved in the procedure of a secure authentication of a registered user to the MSNP are illustrated on Figure 4.3. The user is assumed to be already registered in the MSNP and thus hold the authentication and signing certificates. A user who is member of any group also holds a social certificate. The authentication is in fact a SSLv3/TLS handshake protocol specified in RFC 4366 [BWNH$^+$06]. During the authentication a user needs to provide her valid authentication certificate to the MSNP.

4.4.3 Group creation

The steps involved in the procedure of secure registration of a new social group by a registered user are illustrated on Figure 4.4. The user is assumed to be registered in and authenticated to the MSNP. The user selects a name for the new group and submits the choice to the MSNP. The MSNP updates the database of registered

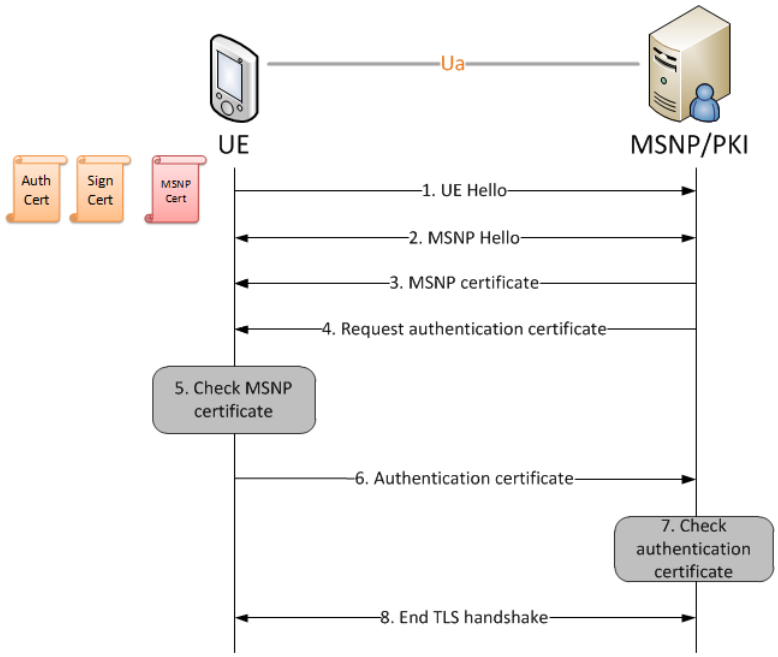


Figure 4.3: The initial SWiN design: User authentication.

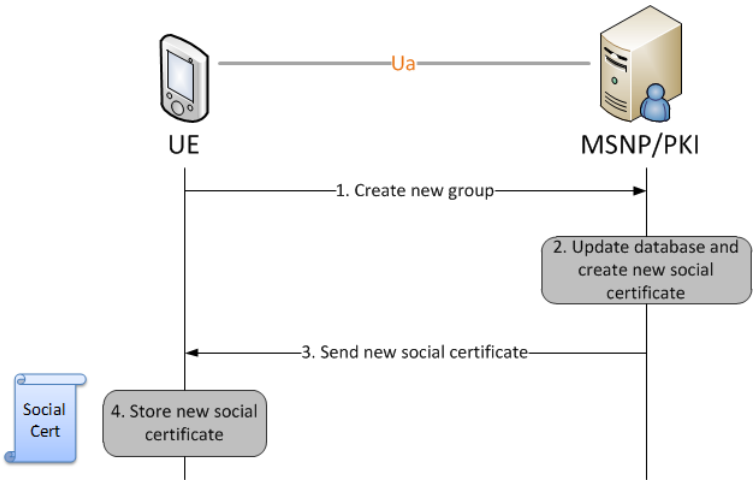


Figure 4.4: The initial SWiN design: Group creation.

groups and group memberships and creates a social certificate for the user who automatically becomes a creator of this group.

Several remarks can be added:

- A social certificate is a structure which must bind the social group a user belongs to and the role of this user within this group, such as creator, moderator, member, etc. The group creator by default becomes the group modera-

tor. Different roles define different rights and privileges of users within social groups.

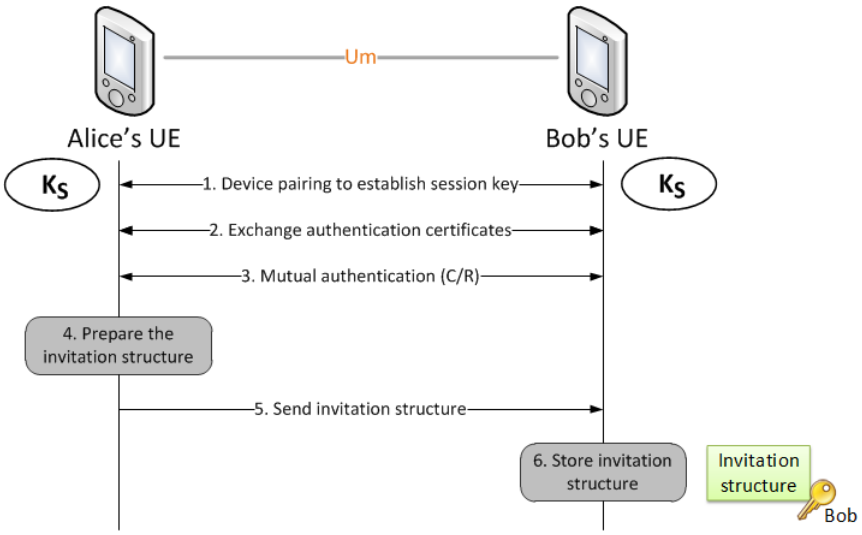
- The central issue related to the functionality supporting the creation of social groups is the format of the issued social certificates. The format of social certificates remains an open issue in the initial design. One solution is to use attribute certificates specified by the X.509v3 standard [FH02]. Another approach which seems to be more flexible and thus effective is to use SAML assertions [CKPM05].
- Another important issue is whether each user holds a single social certificate which stores information about all the user's roles within all the social groups he or she belongs to, or there is a separate social certificate for each social group that the user is a member of. The later is clearly a better solution from the privacy perspective.

4.4.4 Group invitation

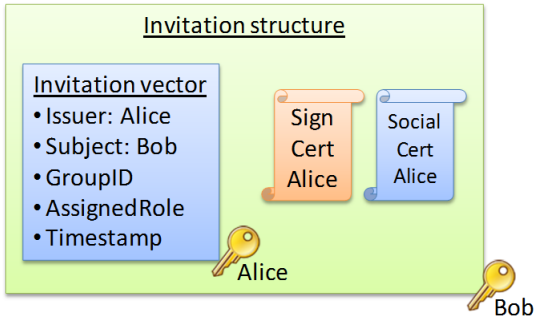
The steps involved in the procedure of invitation of another user to a group by a registered user being the moderator of the group are illustrated on Figure 4.5a. The users first perform device pairing using one of the protocols, described in Section 4.2.3, i.e. ViDPSec or MANA. During the device pairing a session key is generated which is used to encrypt the communication channel. After that the users exchange authentication certificates and perform mutual authentication using public key cryptography and based on challenge/response. The inviting user Alice being the group creator (and thus moderator) is assumed to be registered at the MSNP and hold corresponding authentication and signing certificates, and the certificate of the MSNP. But this requirement is not imposed on the invited user Bob. If Bob is not registered at the MSNP, he should use temporary self-signed certificates but use the same identifier when Bob later registers at the MSNP.

In order to invite Bob the group moderator Alice prepares a special invitation structure and sends it to Bob. The user Bob stores the invitation structure which serves as a proof of his temporal membership within this group before it is officially activated. Temporal membership is valid during a limited period of time (e.g. 24 hours) and means that Bob has only limited privileges and user rights within the group. Bob can activate the invitation to complete the registration process and receive a valid social certificate in order to fully communicate with other members of the group without any constraints. This is done whenever Bob is next time connected to the MSNP. If Bob is a new user who is not registered at the MSNP then Alice could also send the MSNP certificate to Bob so that he can use it in order to verify signatures on social certificates of other group members before he registers himself at the MSNP.

The steps involved in the procedure of invitation activation and obtaining a permanent group membership are illustrated on Figure 4.6. The invited user Bob authenticates to the MSNP and undergoes an optional registration procedure if Bob



(a) Group invitation.



(b) Invitation structure.

Figure 4.5: The initial SWiN design: Group invitation and invitation structure.

is a new user and presents the invitation vector to the MSNP. The MSNP checks and validates the invitation vector, updates the database of group members and creates a new social certificate for Bob.

The format and the contents of invitation structures is a challenging moment in the initial SWiN project design. In general outline, the format of the invitation structure is shown on Figure 4.5b. The invitation structure is encrypted with the public key of the invited user so that only the invited user can read the contents of the structure. The moderator obtains the public key of the invitee during the authentication step. The invitation structure contains the following pieces of information:

1. An invitation vector which is a SAML assertion signed with the private key

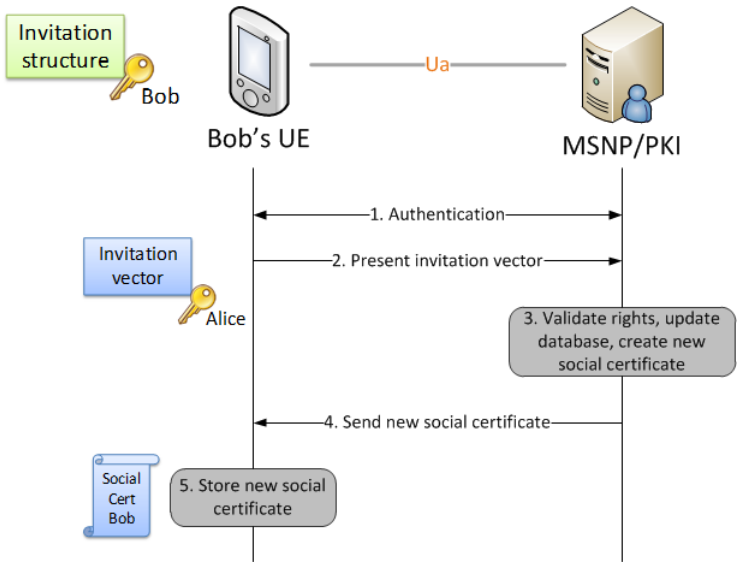


Figure 4.6: The initial SWiN design: Invitation activation.

of the group moderator. The invitation vector includes the following pieces of information:

a) Issuer: The unique identifier of the group moderator Alice.

b) Subject: The unique identifier of the invited user Bob.

c) GroupID: The unique identifier of the group to which a new user is invited.

d) AssignedRole: The role which is to be assigned to the new group member, e.g. moderator, member, etc.

e) Timestamp: To define the validity of the invitation vector.

2. A social certificate of the group moderator Alice so that her moderator's role can be verified by the invitee Bob. This is important to establish a chain of trust through which the temporary membership can be verified.

3. A signing certificate of the group moderator Alice in order for the invitee Bob to verify to the signature of Alice and to check that the invitation vector indeed concerns the desired group and the desired role is assigned.

4.4.5 Mutual role validation

Two users of the same social group can validate roles of each other within this group through the means of direct communication between their mobile devices. Figure 4.7 shows the case in which the user Bob holds only a temporal membership.

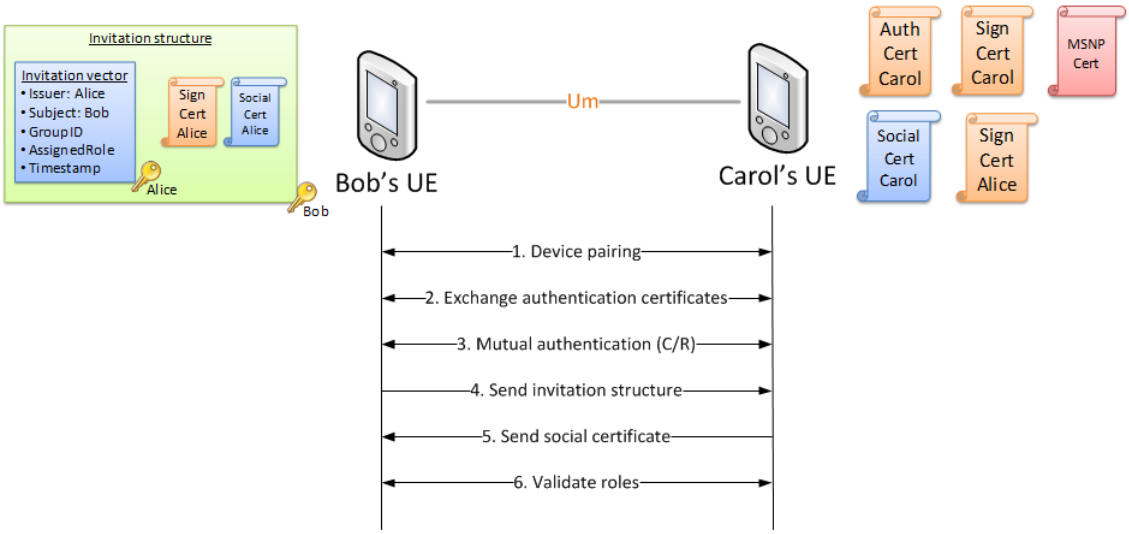


Figure 4.7: The initial SWiN design: Mutual role validation.

Bob holds the invitation structure received previously from the group moderator Alice. The invitation vector as a part of the invitation structure describes the new role of Bob within the group. Another user Carol is a regular member of the social group and thus possesses the social certificate that states her role within this group. Obviously if both users are permanent members of the group, they just simply exchange valid social certificates. In order to authenticate each other both users must use a special client application installed on their UEs. First, users perform device pairing to establish a session key to protect the communication channel. Then users exchange authentication certificates and perform mutual authentication using the public keys based on challenge/response. Next, the user Bob presents his invitation vector instead of the social certificate, while the user Carol presents her social certificate that states her regular membership within the group. Users can now cross validate the roles of each other within the group.

The design and security protection of offline mode functionality is one of the most challenging issues of the present design and several remarks can be added in regards to the offline mode procedures described above.

1. To perform direct mode communication users need to have a special client application installed on their UEs. The application should also allow to keep track of each others' positions. Users are required to install the application before their start direct mode communication. During the client installation users become registered at the MSNP according to the implicit requirement. As a result, users who communicate in offline mode and have a client application pre-installed on their devices should thus hold authentication and signing certificates, and the certificate of the MSNP. However, assume that there is another user who has never heard about the client application but

would like to join the group and start the interaction with the group members. In this situation the moderator of the group can transfer client together with the temporary group membership and the certificate of the MSNP during the invitation procedure. The ability to invite non-registered users widen the functionality of the mobile social network.

2. Another open issue is whether a social group can have several moderators. According to the present scheme, two users who are invited by different moderators cannot authenticate each other because their invitation vectors would be signed with different keys. Thus, the users must wait before they obtain their valid social certificates, to be able to communicate with all members of the group.

3. Finally, to make a scheme more usable it is desirable that all users of a social group should be able to invite users and issue special invitations which require pre-moderation.

It must be pointed out that the listed challenges are left out of the scope of this thesis. In the following chapters, the thesis work focuses on the format of the basic data structures utilized by the suggested design and the protection of identity and group handling through the introduction of user and group pseudonyms. The next chapter describes the motivation for these changes formulated in a problem statement.

Chapter 5

Problem statement and motivation

The chapter forms the problem statement which addresses and illustrates the major privacy aspects of the initial SWiN design to be solved.

The description of the SWiN project secure identification scheme given in Chapter 4 emphasizes a broad use of identifying information. User and group identifiers are included in various basic data structures transferred or exchanged during different communication procedures. If these structures contain real identifiers then it obviously brings a risk to user privacy because it would make it easier for adversaries to detect social relations and group memberships and perform undesirable profiling practices. The solution to increase personal protection of users is to provide a level of anonymity to users of the mobile social network. This can be done through the introduction of pseudonyms. Pseudonyms should replace real identities and be used as identifiers instead. Pfitzmann and Köhntopp [PK01] define two main factors which define the effectiveness of pseudonyms and the strength of anonymity. The ultimate privacy-preserving version of the design with support for pseudonymity services should meet both requirements:

1. It should be impossible to link a pseudonym and its owner. The strength of anonymity decreases with increasing knowledge about the link between a pseudonym and its owner.

2. Pseudonyms should be periodically changed to prevent adversaries from being able to observe any patterns with time. The strength of anonymity decreases with the increasing use of the same pseudonym.

The main goal of the modifications proposed in this chapter is to have an identification scheme in which users remain anonymous towards the MSNP which is considered to be a distrustful entity. The MSNP should know only users' pseudonyms but is able to determine the real identity of users only under special circumstances such as an abuse of a pseudonym for a criminal purpose and only through communication with authorities on the mobile network operator side. Moreover, the pseudonyms should be periodically changed to avoid patterns with time.

Pseudonyms should replace real identifiers in such basic structures as:

1. User authentication certificate (*Subject field* which contains the name of the certificate owner)
2. User signing certificate (*Subject field* which contains the name of the certificate owner)
3. User social certificate (*Subject field* which contains the name of the certificate owner and *Attribute field* which contains group name)
4. Invitation vector (*Issuer field* which contains the name of inviting user or the issuer of the invitation, *Subject field* which contains the name of the user to whom the invitation is issued and *Attribute field* which states the name of the group to which the user is invited.)

In addition, user and group identifiers are needed for a discovery mechanism. A discovery mechanism should enable users to find friends and members of the same social groups in the physical proximity. The search is archived by broadcasting some kind of identifiers which should be recognized only by authorized users. Broadcasting real user and group names leads to no good. The algorithm itself for discovering users is out of the scope of this work.

The following chapter provides a detailed description of the proposed modifications to the design in an effort to address the afore-mentioned problem.

Chapter 6

Privacy enhancing modifications

The chapter defines a number of proposals for modifications and extensions to the design aiming to increase the protection of user identity privacy. The approach is based on introducing pseudonyms for entities in the identification scheme of the mobile social network.

6.1 Pseudonyms for subscriber identification in GBA environment

Before discussing the pseudonyms which would be used within the mobile social network, it is necessary to ensure that the MSNP does not obtain real identities of users during the identification of users in the GBA scheme. As it is mentioned in Chapter 5 the MSNP is assumed to be an untrusted network entity. This means that it should have knowledge neither about the real names of users registered at the portal, nor the real names of social groups created by the users.

According to the standard [3GP10a] "service continuity" can be archived only when the GBA is configured the way that the NAF (the MSNP in the current design) receives from the BSF some kind of user identity information during the bootstrapping usage procedure. In this case the NAF can determine whether the same user contacts the NAF to ensure a continuous service. In other words, the user identity is needed to ensure that the NAF is able to update the keys for a communication over the Ua interface. If no user identity is transferred to the NAF then the user remains anonymous to the NAF and the B-TID functions as a temporary user identifier. But only with B-TID the NAF cannot provide a continuous service because whenever the UE updates they key, it performs bootstrapping, obtains new key and contacts the NAF with a new B-TID value which however cannot help the NAF to determine whether it is the same user that contacted the NAF previously. To ensure service continuity the NAF could receive from the BSF the real identity of a user (e.g. MSISDN, IMSI or IMPU) but such GBA scheme is subject to eavesdropping attacks that uses such mechanisms as IMSI-catcher [Str07]. Thus, if user privacy is desired then the NAF should obtain a user pseudonym rather than the

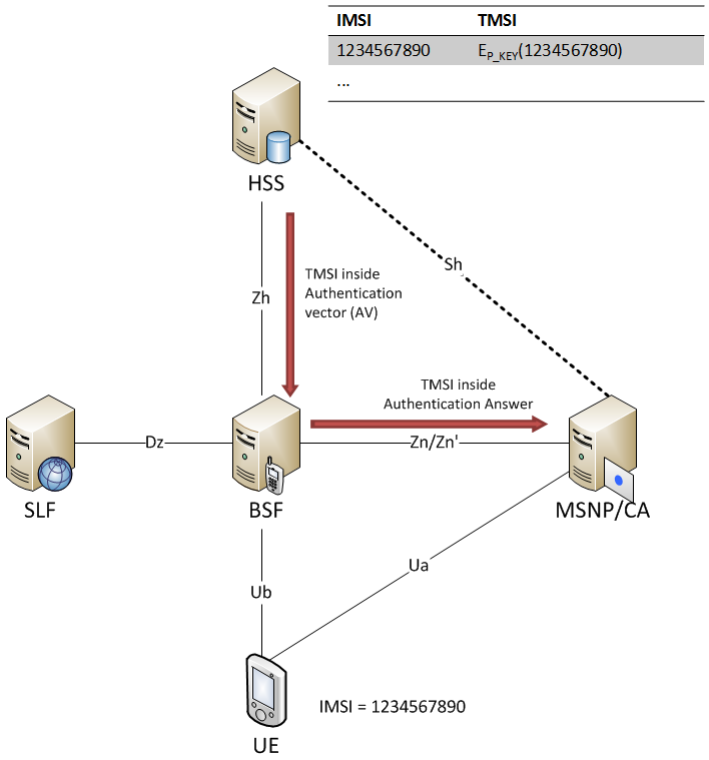


Figure 6.1: Subscriber pseudonyms in GBA environment

real identity. In other words, an important requirement for identity protection in the SWiN design is that the BSF should be configured the way that during a bootstrapping usage procedure the NAF obtains from the BSF a user pseudonym instead of the real user identity. Such configuration of the BSF is possible according to the GBA standard [3GP10a]. This way both service continuity and user anonymity are ensured.

Generation of user pseudonyms takes place at the level of a mobile network operator which actions are assumed to be trusted. The HSS is responsible for creating user subscriber pseudonyms called TMSI in the context of cellular networks (Temporal Mobile Subscriber Identity), binding them with real identities, and assigning a pseudonym to each UE. A mobile device is assigned a TMSI which replaces the device's IMSI when it connects to a base station. The format of pseudonyms used by the HSS to identify its user subscribers is an implementation issue for the HSS. One approach is to generate a pseudonym by encrypting the IMSI with a pre-determined key called pseudonym key, that never leaves the HSS [3GP04]. The pseudonym encrypting (generation) and decrypting (mapping) are internal procedures within the HSS thus the encryption-decryption algorithm can be independent for each HSS and does not need to be standardized. Ideally, the HSS should generate a list of pseudonyms for a user subscriber - one for the use in each separate NAF. The

TMSI structure and mapping with IMSI is discussed in detail in technical specification [3GP11]. Figure 6.1 illustrates how the MSNP in the current design obtains the user pseudonym or TMSI generated by the HSS. First, TMSI is transferred to the BSF from the HSS over the Zh interface along with the authentication vector during the bootstrapping authentication procedure (See Figure 3.6, Step 2). After that according to the BSF policy the BSF includes the pseudonym in the Profile field of the authentication answer which is the response message of the NAF's key request, and sends it to the NAF during the bootstrapping usage procedure (see Figure 3.7, Step 3). For more details on bootstrapping authentication and usage procedures see Section 3.2.1.

Although the 3GPP standard [3GP10a] does not discuss whether the NAF can obtain the real user profile information corresponding to a given pseudonym from the HSS directly there are several additional papers that ponder over it. [3GP04] proposes that the NAF uses the Sh interface to retrieve the real user profile information from the HSS belonged to the pseudonym. The Sh interface is generally available only for IMS based applications, but any GBA scheme can be extended to support it.

6.2 Functionality with support for pseudonyms

Section 6.1 describes the need for pseudonyms generated at the mobile network operator level and transferred to the MSNP during the authentication of a user to the MSNP in the bootstrapping scheme. Such pseudonyms generated by the HSS and described above are referred from now on to as *global user pseudonyms* or *TMSI* and appear inside *Profile* field of the authentication answer in the schemes below. However apart from these pseudonyms, there is a need to introduce another type of user and group pseudonyms to be used locally within the mobile social network. These pseudonyms should identify users or groups to the MSNP and appear in basic data structures replacing real identities. Such pseudonyms are referred to as *local user and group pseudonyms* and appear as *PID* in the schemes described below. In the following text, data structures, such as certificates and invitations, in which real user and group identifiers are replaced with valid local user or group pseudonyms, are referred to as anonymous data structures.

According to the design description given in Chapter 4, the MSNP is responsible for issuing user authentication and signing certificates as well as for issuing user social certificates. Since authentication and signing certificates follow X.509 v3 format the issuance of anonymous certificates may take place according to the scheme described in RFC 5636 (see Section 3.2.3). The present work proposes two versions of the registration procedure. Anonymous social certificates are SAML assertions and issued by an assertion module at the MSNP side. Anonymous invitation structures are generated at the client side as SAML assertions.

6.2.1 Pseudonym generation algorithm

The generation of local and group pseudonyms should be performed on the client side. There can be several approaches. For example, a user or group pseudonym can be generated by either applying a salted hash function or a keyed hash function over the real name of the user or group. In this chapter the algorithm for pseudonym generation is chosen to be based on a salted hash function. Assume that the real name of a user is Alice. To generate a pseudonym, Alice first selects a random value called salt S_A and then calculates a publicly known hash function over the real name of the user concatenated with the salt value, i.e. $PID_A = H(Alice||S_A)$. Alice would share the salt value S_A only with authorized users, e.g. with friends or with members of groups she belongs to, but never with the MSNP. Thus, the MSNP stores the pseudonym of Alice but never has the knowledge about neither the the real name of Alice nor the salt value S_A.

When Alice wants to reveal her identity to another user Bob she would send to Bob her pseudonym PID_A in clear text and a pair $< Alice, S_A >$ encrypted with the public key of Bob where Alice is the real name and S_A is the secret salt value. Only Bob would be able to read the encrypted values. To verify the identity of Alice, Bob would calculate her pseudonym and compare with the pseudonym that Alice claims to hold. If the check is successful then Bob stores a record in his local database $< Alice, PID_A >$ which links Alice to her pseudonym S_A. So whenever Bob sees a pseudonym PID_A he would understand that it is Alice. Salt values can be also changed periodically to prevent patterns. Change of salt values directly entails change of pseudonyms.

The cryptographic hash function H however must be strong enough to withstand all known types of cryptanalytic attacks and possess the following properties [Bis04]:

1. **Preimage resistance.** Given a pseudonym PID_A and the knowledge about the hash function H, it should be infeasible to find another name Eve and salt value S_E, such that $H(Eve||S_E) = PID_A$.

2. **Second preimage resistance attack.** Given a real name Alice and salt value S_A and the knowledge about the hash function H, it should be infeasible to find another name Eve and salt value S_E, such that $PID_A = H(Alice||S_A) = H(Eve||S_E) = PID_E$.

3. **Collision resistance.** Given the knowledge about the hash function H, it should be infeasible to find two different $Alice||S_A$ and $Eve||S_E$, such that $PID_A = H(Alice||S_A) = H(Eve||S_E) = PID_E$.

As an alternative, a keyed hash can be used [Bis04], [KBC97]. For example, a pseudonym of Alice can be calculated as $PID_A = HMAC(K_A, Alice)$, where K_A is a secret key shared by Alice only with authorized users.

6.2.2 Format of basic data structures

As it has been mentioned in Chapter 4 that provides the description of the initial secure identification design, the format of the basic data structures has been an open issue. With the introduction of pseudonyms it is important to reconsider the format of such structures and select the most effective one(s). Based on the following proposals for modifications the format data structures has been chosen as follows:

1. User authentication and signing certificates keys should follow X.509 v3 standard [CSF+08]. These certificates are obtained by a user from the MSNP during the registration procedure or whenever the certificates are expired or revoked. The certificates serve the purpose to bind the user's identity (or pseudonym) to the corresponding public key.

2. The format of social certificates and invitation vectors is defined according to OASIS SAML standard [CKPM05]. In fact, both a social certificate and an invitation vector represent an assertion of group membership. However there are two main differences between them. Examples of a social certificate and an invitation vector are given in Appendix A and B.

    a) A social certificate is generated and signed by the MSNP, i.e. the Issuer field refers to the MSNP. A social certificate is generally valid for a limited period of time (e.g. Validity field equals one week). It can be renewed as long as a user has a group membership or revoked such as when a user leaves a group.

    b) An invitation vector is generated and signed by the inviting party, i.e. the Issuer field contains the identity (or pseudonym) of the inviting user. An invitation vector has a short lifetime specified by the parameters in the Validity field.

6.2.3 User registration

A new user registration procedure is divided into two phases. *The first phase* includes the authentication of the UE to the MSNP based on the GBA scheme. *The second phase* of the registration is issuance of user anonymous authentication and signing certificates in X.509 v3 format containing user pseudonyms instead of real user identities.

The present thesis suggests two alternative versions of the scheme for new user registration procedure. The first phase (Authentication phase) of both approaches is the same and is similar to Steps 1-9 in the description of the new registration procedure in Section 4.4.1 with the exception of one important remark. An additional requirement is put on the procedure of fetching the session key material by the MSNP from the BSF. According to the discussion in Section 6.1, to ensure the service continuity and user identity protection the MSNP must obtain a global

pseudonym or TMSI (generated by the HSS). The user global pseudonym is transferred to the MSNP inside the *profile* field of the authentication answer from the BSF. Figure 6.2 and Figure 6.4 illustrate the Authentication phase of the two approaches. The second phase (Anonymous certificate issuance) is however different for two approaches.

Assume that a new user would like to be registered at the application server NAF. If the registration is based on issuing a special authentication certificate to the user which he or she could later on use to get authenticated to the system, then the network architecture should combine GBA and SSC standards.

User registration (Version #1)

The first version (Version #1) of the scheme (see Figure 6.3) requires the involvement of the RA that resides on the side of the MNO in the procedure of anonymous certificates issuance. This approach utilizes the model proposed in the RFC5636 document [PPW+09] and described in Section 3.2.3. The approach assumes that the RA and CA are managed by different organizations and must cooperate to issue anonymous certificates. In this version of the registration procedure, the MSNP plays role of a Certification Authority (AI in RFC 5636 terminology) and the BSF performs the role of a Registration Authority (BI in RFC 5636 terminology). In addition, each user is required to contact the MNO prior the registration in order to request and obtain two tokens: AuthToken for anonymous authentication certificate and SignToken for anonymous signing certificate.

User registration (Version #2)

The second version (Version #2) of the scheme (see Figure 6.5) is a light version of the registration procedure since it does not require any involvement from the side of the MNO and the MSNP performs roles of both the RA and CA.

6.2.4 User authentication

The procedure of user authentication to the MSNP is the same as the procedure described in Section 4.4.2. The only modification is that during the TLS handshake a user provides the valid authentication certificate which contains the user's PID in the Subject field instead of the real identity of the user.

6.2.5 Group creation

Figure 6.6 illustrates the scenario in which user Alice wants to create a new group called SICS. Assume that Alice is a registered user and is known to the MSNP as PID_A. The user first authenticates herself to the MSNP using her anonymous authentication certificate as described in Section 6.2.4. Then she requests to create a group with name PID_{SICS} where PID of the group is calculated according to the algorithm described in Section 6.2.1, i.e. $PID_{SICS} = H(SICS||S_{SICS})$. The

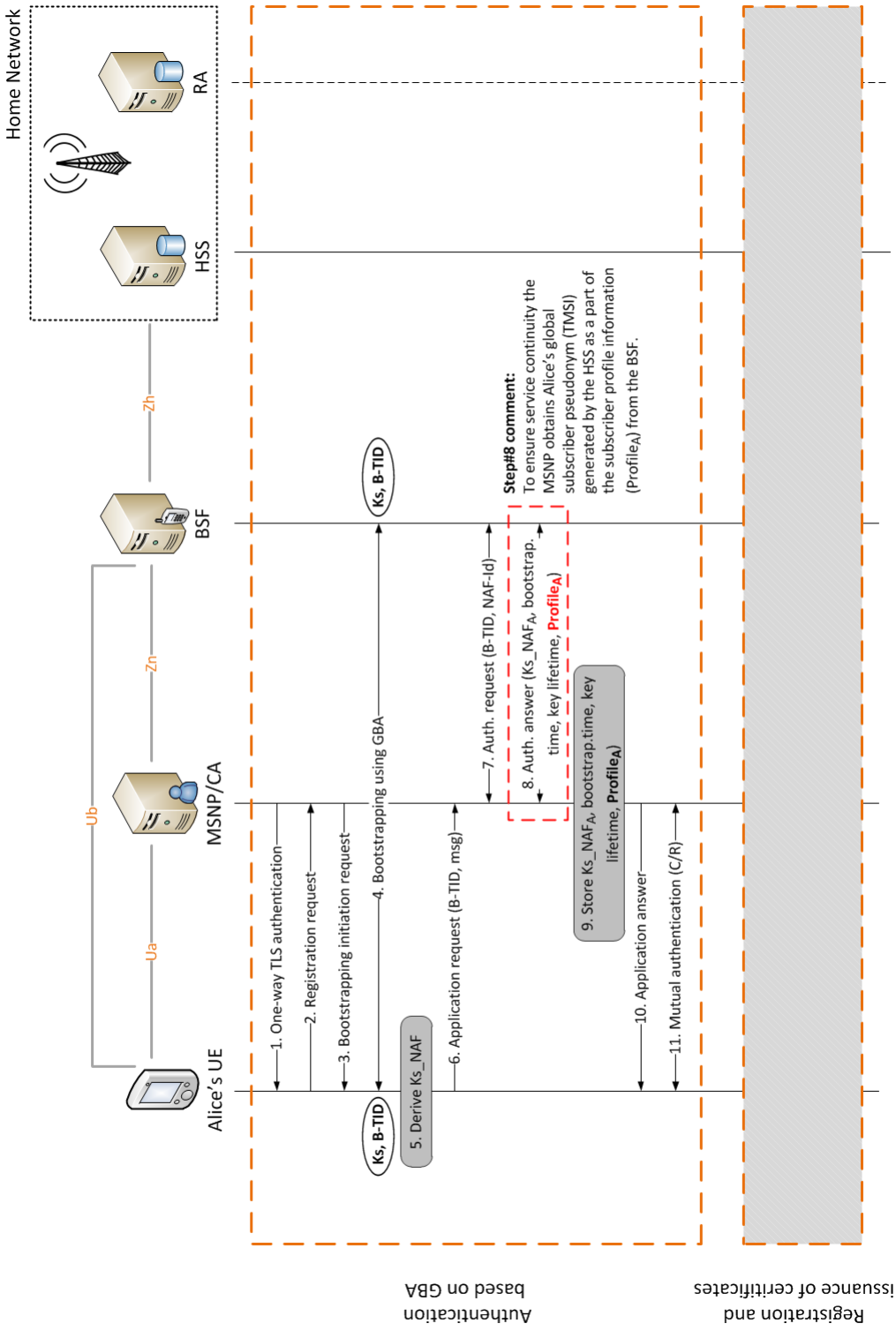


Figure 6.2: The privacy-enhanced SWiN design: User registration (Version #1): Authentication based

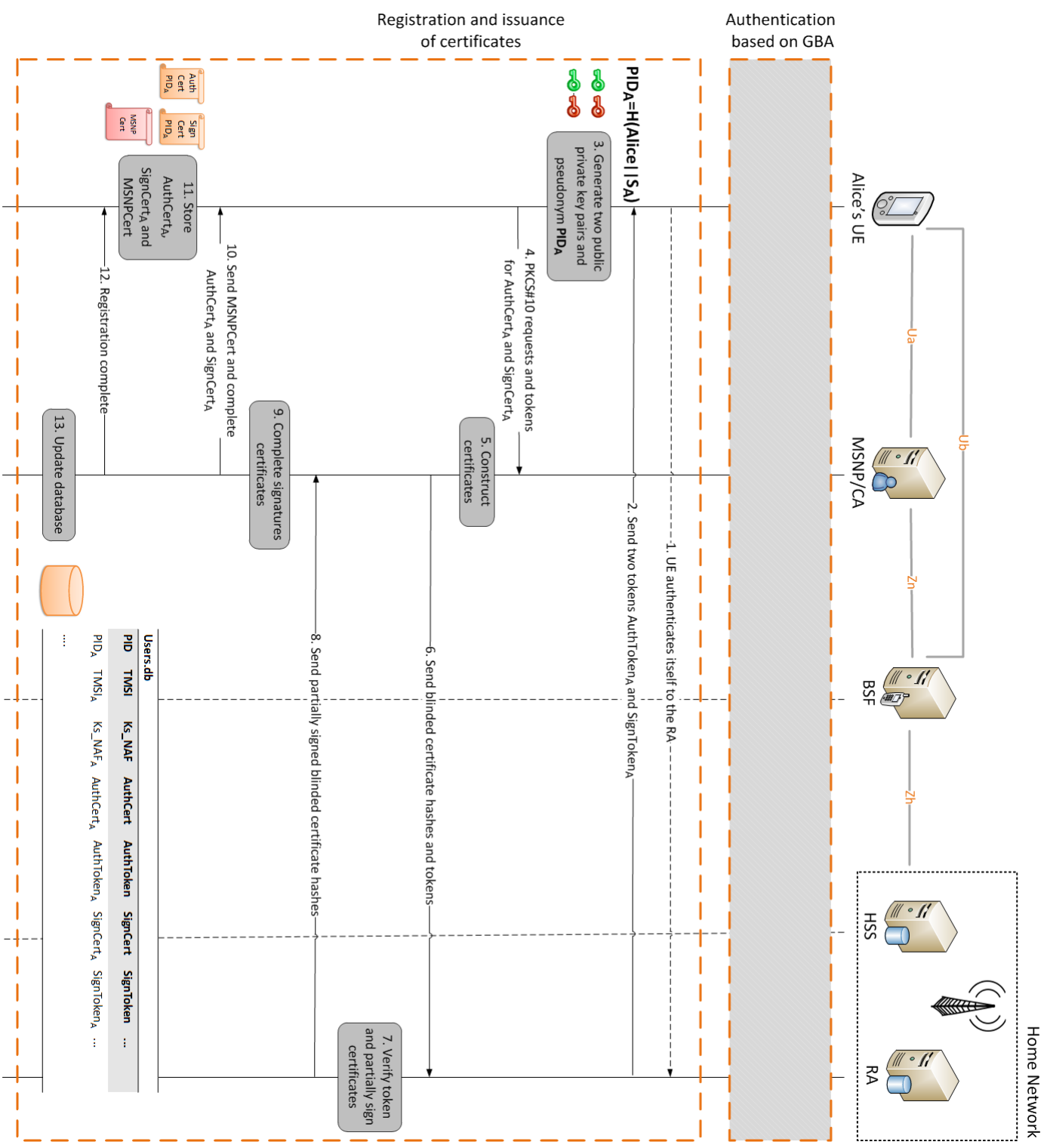


Figure 6.3: The privacy-enhanced SWiN design: User registration (Version #1): Anonymous certificates issuance phase

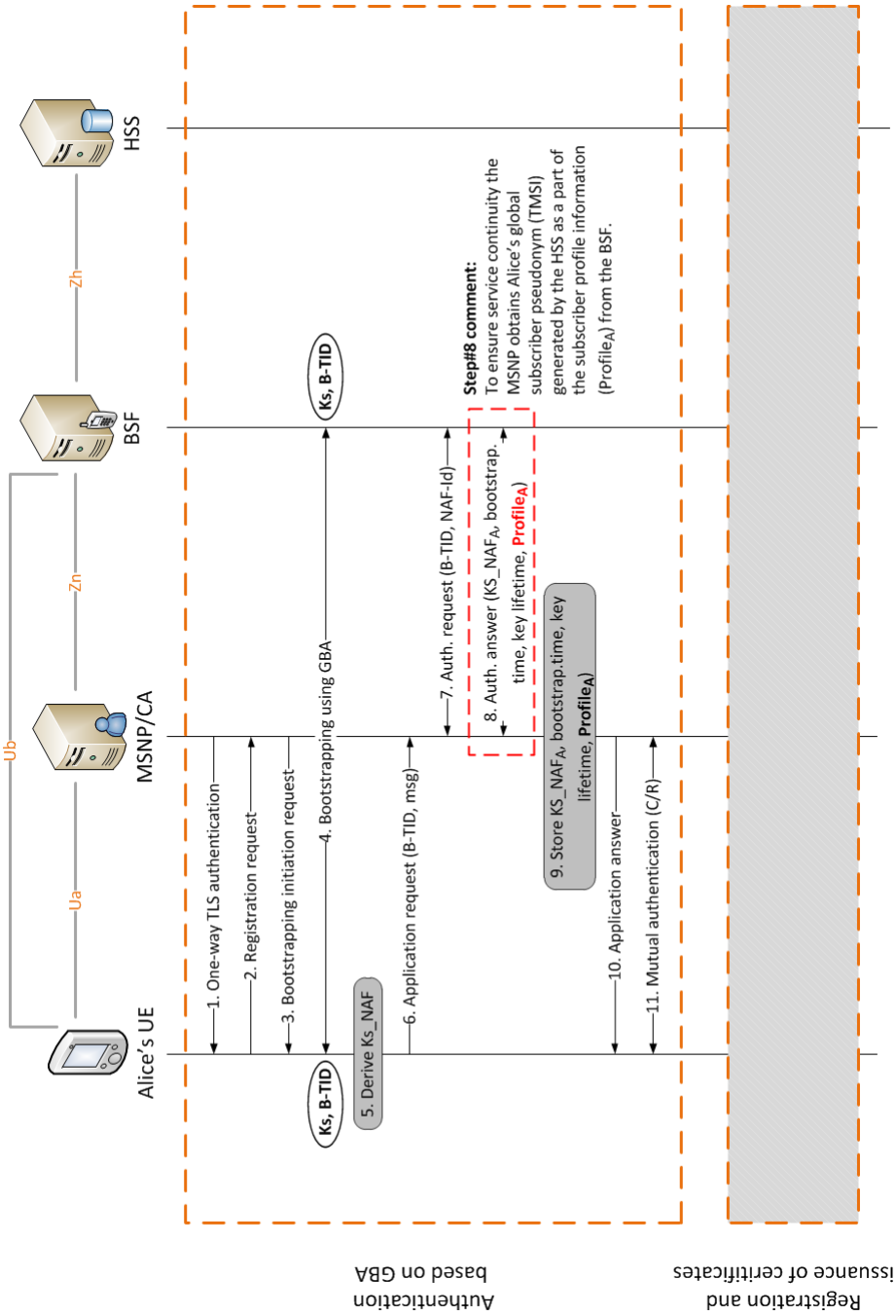


Figure 6.4: The privacy-enhanced SWiN design: User registration (Version #2): Authentication phase

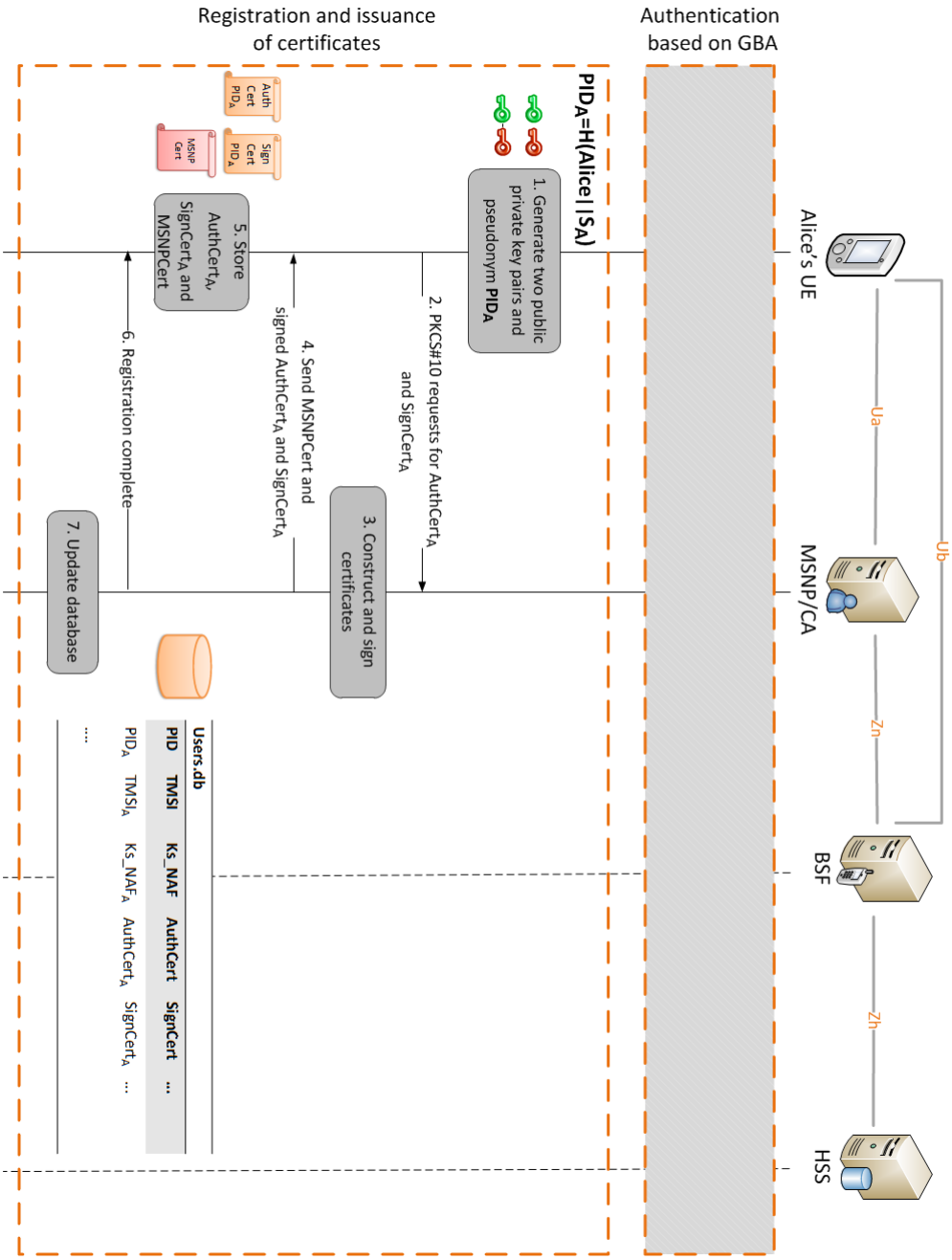


Figure 6.5: The privacy-enhanced SWiN design: User registration (Version #2): Anonymous certificates issuance phase

MSNP adds information about the new group in its database. From now on it only knows that the user PID_A is administrator of the group PID_{SICS}. The MSNP also issues a new social certificate for Alice. An example of a social certificate of Alice that states her role as administrator in group PID_{SICS} is given in Appendix.

Social certificates are issued and signed by the MSNP. It should be noted that in case Version #1 of the new user registration procedure is used then there is a need to introduce an additional scheme for digital signature for the MSNP to sign social certificates because the MSNP should be able to sign certificates without any involvement of the RA. It would also require a user to hold two public key certificates of the MSNP: one to verify the threshold digital signature on user authentication and signing certificates signed in the cooperation by the RA and CA, and one to verify digital signature on social certificates signed by only the MSNP. If Version #2 is utilized then the MSNP can use the same private key to sign social certificates.

6.2.6 Group invitation

While groups can be created by any registered user, only authorized group members can invite new members. To allow flexibility for group handling procedures basic user roles within a group are defined as follows:

1. **Creator** can edit or delete the group, as well as assign group moderators. Creator is a moderator by default.

2. **Moderator** can invite new members to join the group.

3. **Member** is a permanent group member who possesses a valid social certificate signed by the MSNP.

4. **Temporary Member** is a user who has been invited to a group but has not activated the invitation at the MSNP to become a permanent member yet. Such user possesses a valid invitation vector signed by an authorized moderator which functions as a temporary social certificate. A temporary user has a short life time and might have limited communication privileges.

Assume the user Alice is a creator (thus a moderator by default) of the group SICS and she invites the user Bob to join the group. Both users are registered at the MSNP and hold the corresponding user authentication and signing certificates. The MSNP knows Alice as PID_A and Bob as PID_B. Alice also holds a social certificate issued and signed by the MSNP that states her role as creator within the group PID_{SICS}. Assume that Alice and Bob have never communicated previously and neither Alice nor Bob knows the real identities of each other. Thus, before Alice invites Bob they first need to authenticate each other and reveal their real names to each other. Figure 6.7 illustrates that first the users perform device pairing using one of the protocols described in Section 3.2.2 to establish a session key for the protection of the communication channel between them. The users then exchange their authentication certificates and perform public key cryptography based

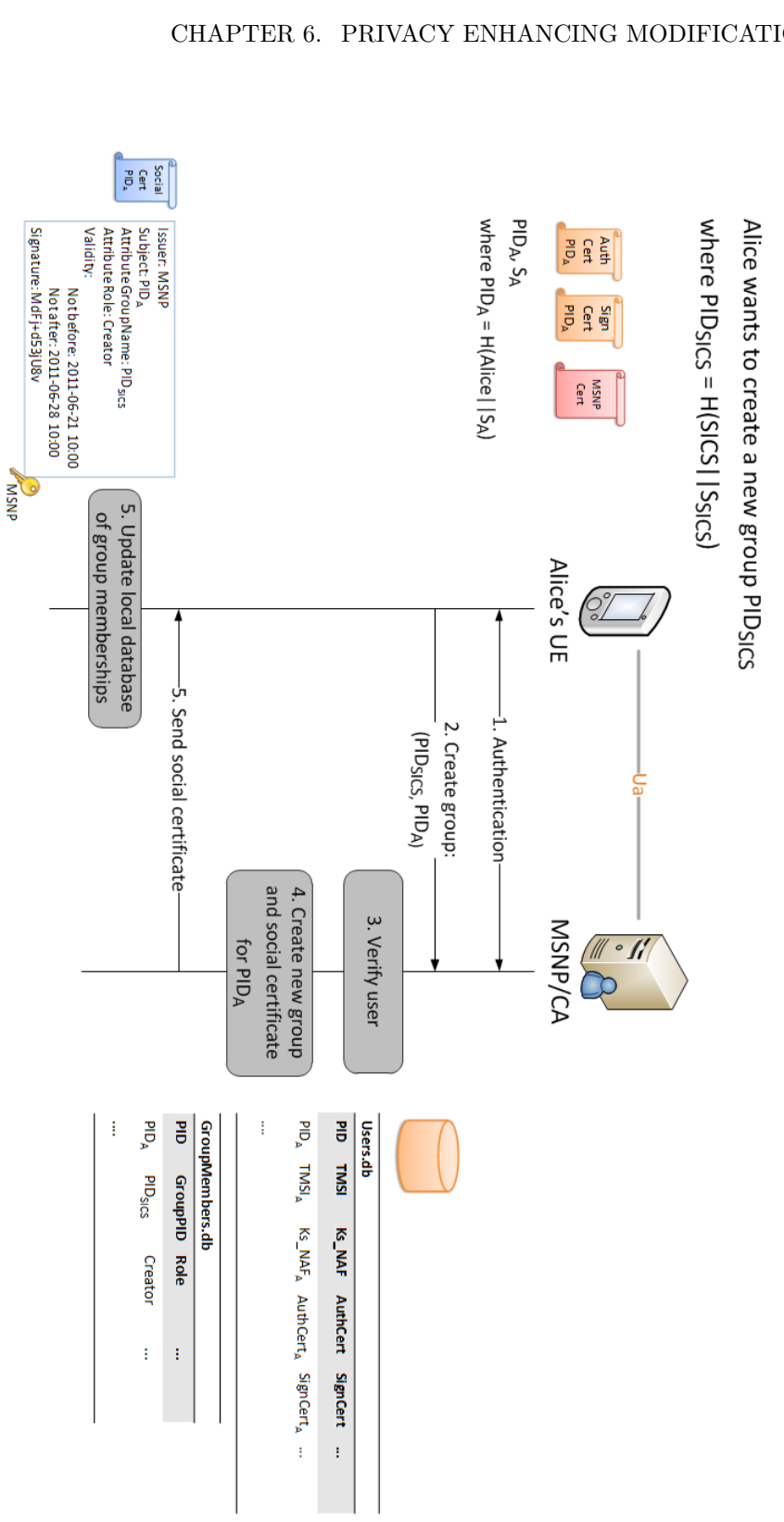


Figure 6.6: The privacy-enhanced SWiN design: Group creation.

authentication. After the mutual authentication is done the users can optionally obtain the knowledge about the link between the pseudonym and the real name of each other. To reveal her identity, Alice sends to Bob a structure that contains the following fragments:

1. The real name *Alice* and the salt value S_A encrypted with the public key of Bob, and the pseudonym PID_A, all together signed by PID_A who is the moderator Alice.

2. The signing certificate of Alice, namely $SignCertPID_A$.

Bob sends a similar structure to Alice to reveal his identity to Alice. After Alice knows the pseudonym of Bob and is assured that the user that hides behinds this pseudonym and communicates on behalf of this pseudonym is indeed Bob, Alice prepares and sends an invitation structure that consists of:

1. An invitation vector (inVector) in SAML format which states the role of the newly invited user PID_B as a temporary member. The invitation vector is issued and signed by PID_A - the moderator of the group PID_{SICS}.

2. The real name of the group SICS and the salt value S_{SICS} for pseudonym calculation check also encrypted with Bob's public key.

3. The social certificate of the moderator PID_A so that it is possible to verify that the invitation was issued by an authorized moderator of the group.

Upon the recipient of the invitation structure from Alice, Bob performs checks to verify that Alice is indeed the moderator of the group SICS and that the invitation vector contains correct information. After that there are two possible scenarios. Bob can either activate the invitation by contacting the MSNP and presenting the invitation vector from the invitation structure, if Bob has a connection to the MSNP, or otherwise Bob can start directly communicating with other group members holding a status of a temporary member.

Figure 6.8 illustrates the procedure of invitation activation. Bob authenticates himself at the MSNP as PID_B as described in Section 6.2.4 and presents to the MSNP the invitation vector which is an extraction from the invitation structure that Bob received from Alice. The invitation vector is signed by Alice but the signature appears as a signature by PID_A, the user which is registered with the MSNP and the user that the MSNP knows as the creator of the group PID_{SICS}. The MSNP needs to verify all this information and if correct sends in response a new social certificate for Bob which states the role of Bob as member and is issued and signed by the MSNP.

6.2.7 Mutual role validation

If it is not possible for Bob to immediately activate the invitation, e.g. due to a lost connection to the MSNP or expensive roaming costs, Bob can nevertheless start

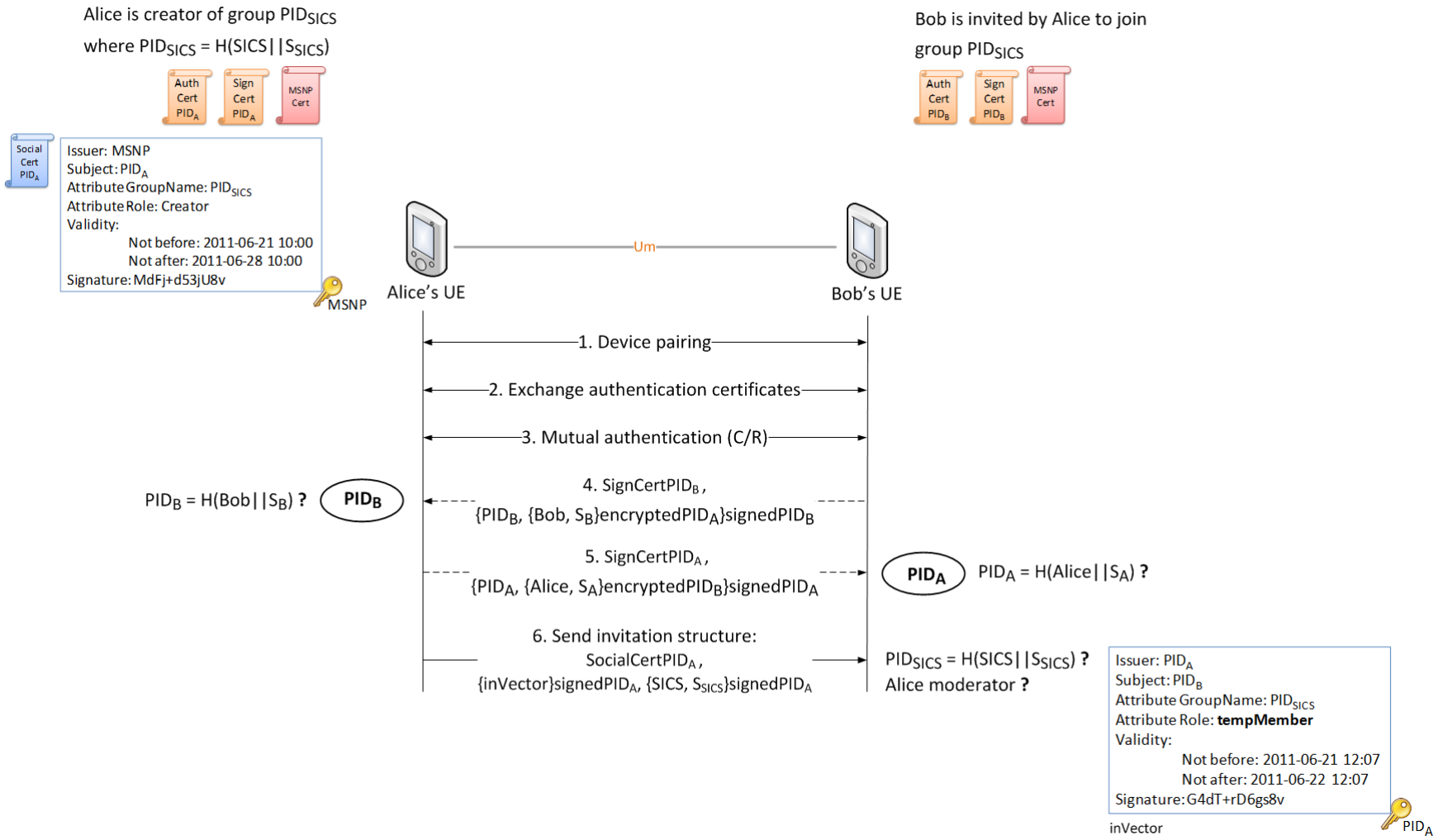


Figure 6.7: The privacy-enhanced SWiN design: Group invitation.

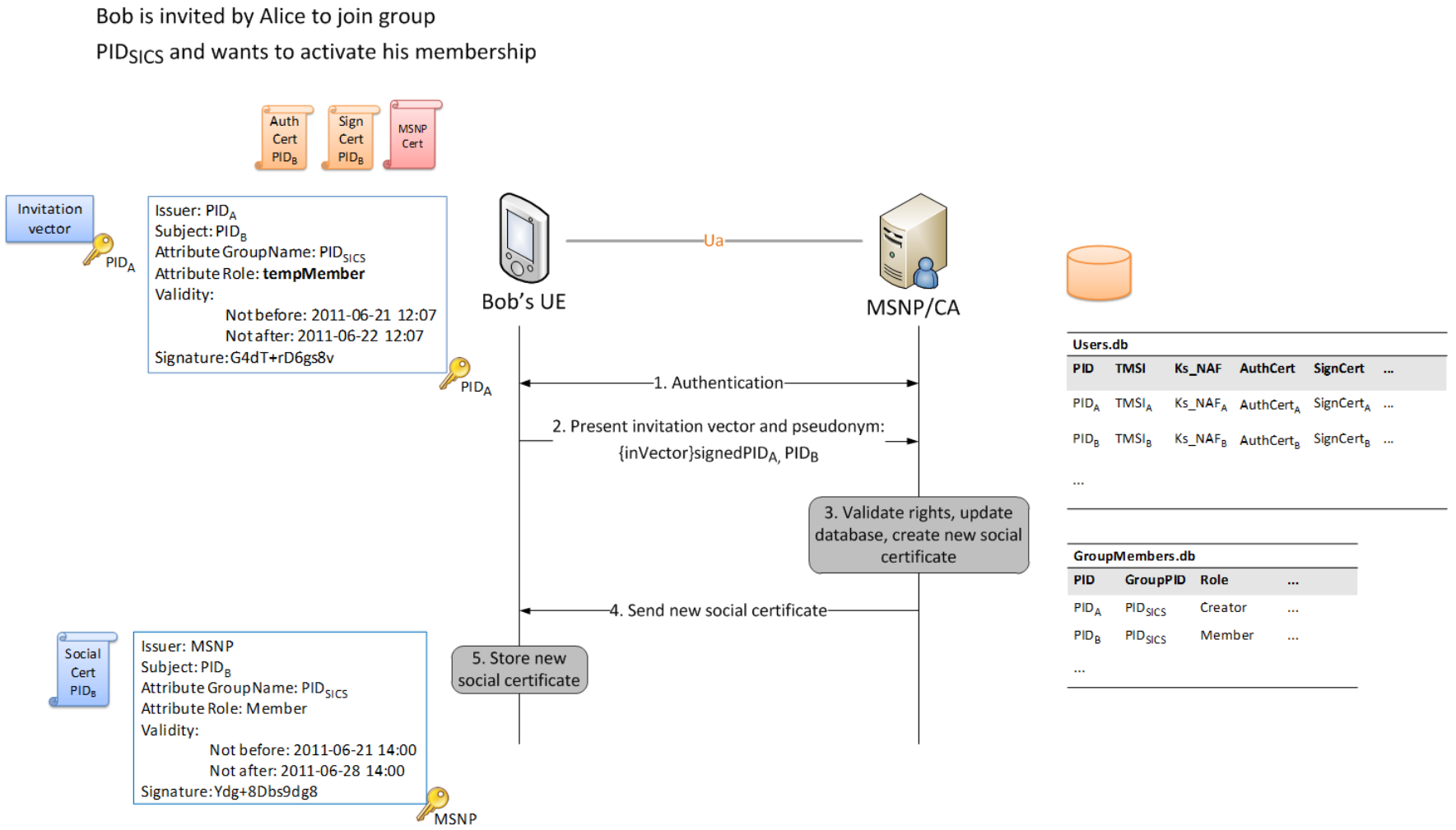


Figure 6.8: The privacy-enhanced SWiN design: Invitation activation.

communicating with other members of the social group but with limited communication privileges and holding a status of a temporary group member. Prior the communication with another member of the group Bob and another member would need to mutually validate the roles of each other.

Figure 6.9 illustrates the procedure of mutual role validation between Bob who is a temporary member and holds the invitation vector obtained during the invitation procedure from PID_A and Carol who is a permanent member of the group PID_{SICS} and holds a valid social certificate issued and signed by the MSNP. First of all, users perform mobile device pairing to establish the session key. Then they exchange authentication certificates and perform mutual authentication using public keys and the challenge/response scheme. After the mutual authentication is complete, the users can optionally exchange special information structures to reveal their real identities they hide behind their pseudonyms (Steps 4 and 5 in Figure 6.9 are similar to Steps 4 and 5 in Figure 6.7). Finally, they exchange data structures which show their roles within the same group PID_{SICS}. Bob presents the invitation vector signed by the moderator PID_A and the social certificate of the moderator PID_A. Carol sends her social certificate $SocialCert_C$. Now Bob can verify the role of Carol by looking at her social certificate. Carol in turn can verify that the invitation was issued by an authorized moderator PID_A, that the signature of PID_A on the invitation vector is valid and that the lifetime of the invitation vector has not expired yet. After validating roles of each other, users can start communicating.

6.3 Pseudonym renewal procedure

The renewal of pseudonyms should take place at the level of the MNO which means that the HSS should periodically assign new pseudonyms for subscribers, and at the mobile social network level, which means that user clients should be configured the way that the salt value changes with time. The validity of old and new pseudonyms can overlap to ensure that there is a transitional period when both pseudonyms are valid to ensure a smooth transition to new pseudonyms.

Bob holds the status of a temporary user in PID_{SICS}. Carol is a permanent member in PID_{SICS}. Both users would like to validate their roles within the same social group.

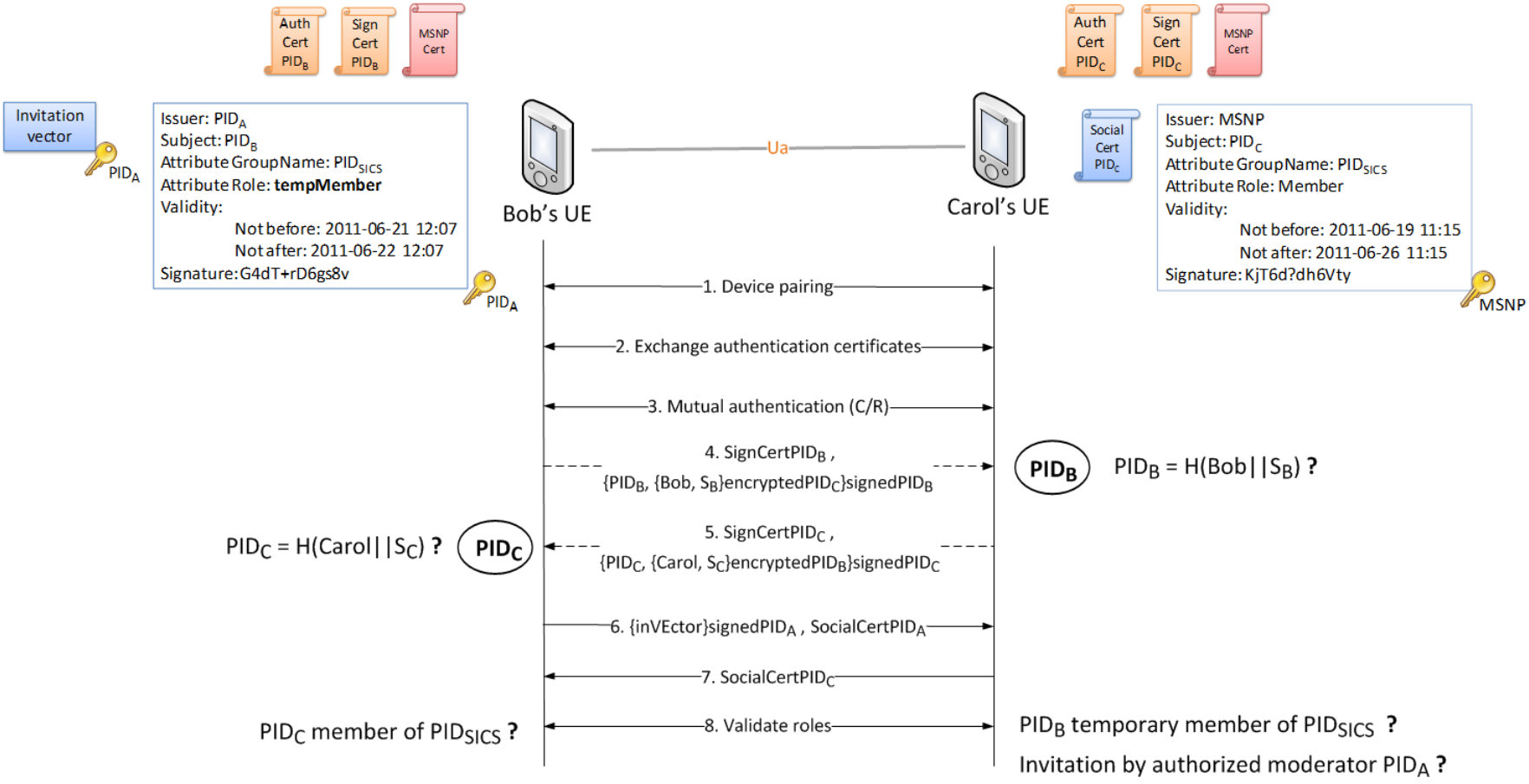


Figure 6.9: The privacy-enhanced SWiN design: Mutual role validation.

Chapter 7

Design evaluation

The chapter provides an evaluation of the privacy-enhanced SWiN project design.

Figure 7.1 demonstrates two versions of the final SWiN architecture design with support for user and group pseudonymity [SO11]. The major components of both schemes are the Client, the MSNP and the MNO. The first scheme 7.1a corresponds to the design in which the user registration procedure is based on the model described in RFC5636 (see Section 6.2.3). In this scheme the RA and CA responsible for issuance of anonymous user certificates are managed by different organizations, i.e. the MSNP acts as a CA and the MNO as a RA. The second scheme 7.1b corresponds to the design that uses the light version of the user registration procedure (see Section 6.2.3). This scheme does not require any involvement from the side of the MNO and the MSNP performs roles of both the RA and CA.

7.1 Comparison of two design versions

The first version of the design that utilizes Version #1 of the registration procedure (see Section 6.2.3) is considered to be more secure since the only trusted entity in the scheme remains the MNO. In this scheme, the MSNP has no knowledge about the real names of users and groups registered at the portal. Moreover, the binding between the global pseudonym (TMSI) and the local pseudonym (PID) of a user is validated during the registration procedure at the network operator side. The validation is carried out by means of technical means of threshold cryptography for digital signature scheme and blind signing technique [PPW$^+$09]. In the second version of the design which utilizes Version #2 of the registration procedure (see Section 6.2.3), the MSNP is still trusted but only in the context of the binding between the global pseudonym (TMSI) and the local pseudonym (PID) of a user. Although the first scheme is more secure and effective in terms of identity protection, it is more cumbersome if compared to the second scheme. The involvement of the MNO in the registration procedure burdens the MNO to validate all user registrations which makes the design heavier.

7.2 Principle design changes

The changes illustrated in Chapter 6 improve the SWiN initial design of the mobile social network described in Chapter 4 by providing support for pseudonymity which in turn allows for identity protection and user anonymity. The principle changes can be summarized as follows:

1. Two levels of pseudonyms are introduced: global pseudonyms which are mobile subscriber pseudonyms (TMSI) generated at the network operator side and local user and group pseudonyms (PID) to be used within the mobile social network and generated by users. The binding between a global and a local pseudonym of a user is performed at the MSNP. The first design version offers additional validation of the correct binding at the MNO side.

2. The modified design requires the usage of pseudonyms on GBA level as an important part of identity. The requirement guarantees the anonymity provided by local pseudonyms.

3. Local user and group pseudonyms are generated at the client side. The cryptographic hash function for pseudonym generation is based on salt values and thus should withstand all known types of cryptanalytic attacks and reduce the chances of impersonation attacks. Revealing of real user and group names happens only in person during a direct mode communication between users, thus, reducing chances for attacks. In addition, during user registration and group creation the MSNP verifies whether there is no other user or group registered under the same pseudonym.

4. In the modified design the trust in the MSNP is diminished. After the introduced changes the MSNP has no knowledge about the real identities of users and groups that are registered at the MSNP. The MSNP only binds global pseudonyms (TMSIs) with local pseudonyms (PIDs) used within the network. In Version #1 (see Figure 7.1a) the network operator remains the only trusted entity. In Version #2 (see Figure 7.1b) the MSNP is only trusted for correct binding.

5. Basic data structures such as user certificates and membership assertions contain only user and group pseudonyms (privacy-preserving identifiers) and thus can be securely transferred over the network.

6. The use of anonymous certificates in X.509 v3 format in which the Subject field contains user pseudonyms instead of real identifiers is introduced for user authentication and signing certificates.

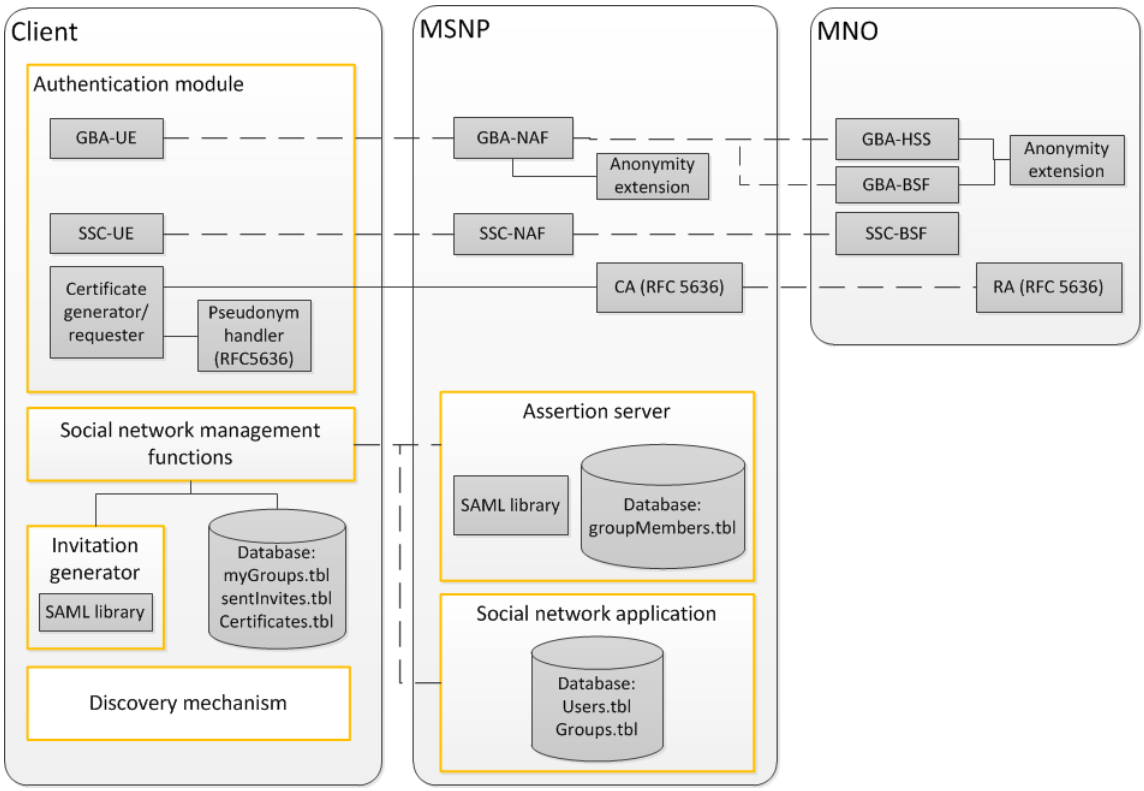
7. SAML standard with support for the use of pseudonyms inside SAML assertion structures is proposed to represent membership assertions, i.e. social certificates and invitation vectors.

8. User group roles are defined as: creator, moderator, member, temporary member.

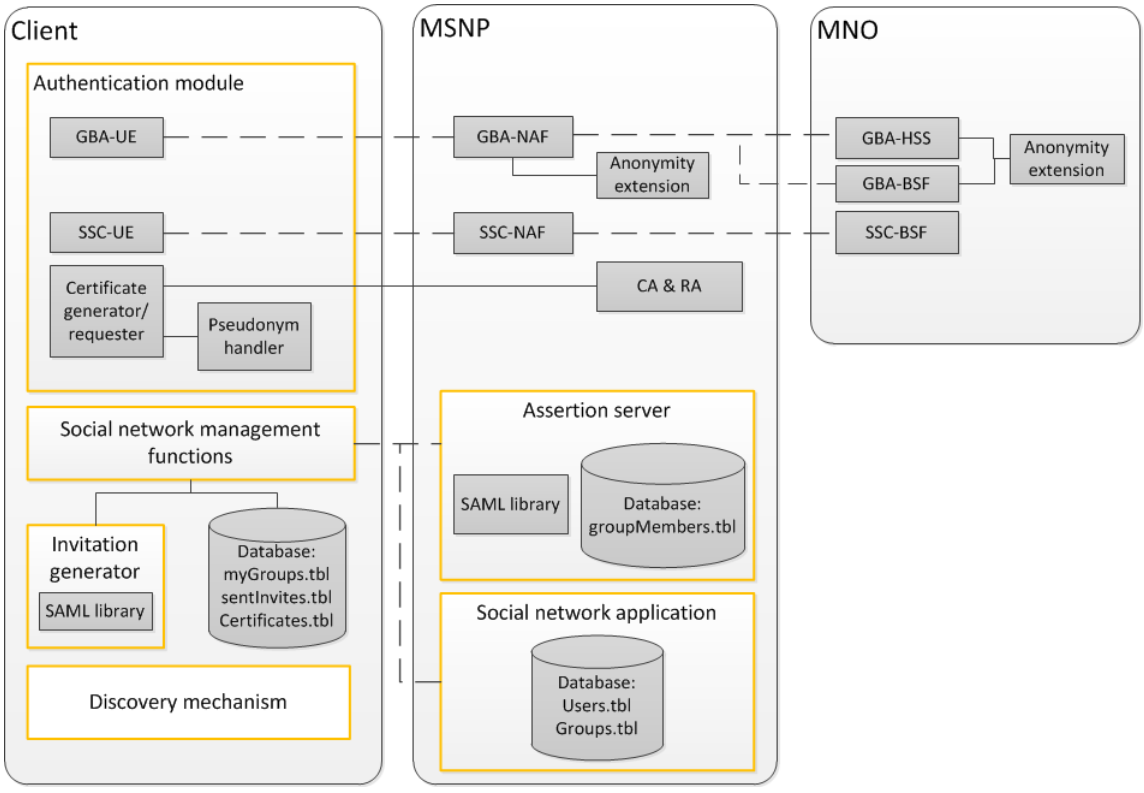
7.3 Open issues

Issues which remain open after the present study can be summarized as follows:

1. The complexity of hash function for pseudonym generation is not studied.
2. In close vicinity it is easy for an adversary to determine the pseudonym of a user by passively monitoring the network and by being familiar with all the parties who communicate.
3. Scenarios of user and group pseudonym renewal procedures are not studied.
4. The problem of having several moderators in the same group is not addressed. How fast can the information about a new moderator propagate among the group members? Which constraints does it add in case two temporary members cannot validate each other's roles due to the fact of being invited to the group by different moderators?



(a) Architecture design: Version#1.



(b) Architecture design: Version#2.

Figure 7.1: Two versions of the modified SWiN architecture design [SO11].

Chapter 8

Conclusions and future work

8.1 Conclusions

The Master's thesis covers the privacy aspects of the secure identification design proposed within the project "Social Wireless Network Secure Identification" carried out in collaboration between SICS, Ericsson and Sony Ericsson. The thesis provides thorough details and understanding of the technologies that enable the architecture design of the novel mobile social network and particularly addresses the privacy issues and challenges related to its identity management. Two major contributions are given to the SWiN project during the work on the present thesis. The first contribution is a broad theoretical study on privacy in the context mobile social networking (Chapter 3). The second contribution is the proposal for changes to improve the privacy preserving capability of the mobile social network. The proposed modifications are based on the evaluation of the initial design against potential risks and threats to user identity privacy (Chapter 4-6). The design improvement is achieved through enhancing identity management by introducing user and group pseudonyms to remove the use of real identifiers within the mobile social network.

The work on the thesis is divided into several phases which are carried out according to the research goals outlined in Section 1.4: 1) theoretical background studies, 2) evaluation of the initial design of the mobile social network and problem statement formation, 3) proposal for modifications, and 4) evaluation of the ultimate privacy enhanced design. All the research goals are archived during the thesis project.

The theoretical background of the thesis work covers two major blocks of studies: overview of mobile social networking with a focus on related privacy issues and the study of the core technologies on which the SWiN secure identification design for a mobile social network is built. The background studies start from looking at different approaches to privacy analysis in social networks. Different architectures of social networks, e.g. centralized and decentralized models, are studied and related advantages and challenges are discussed. A number of research projects aiming to improve privacy protection and create a privacy-preserving social net-

work are analyzed and compared. Next, the move of social networks into mobile space is observed. The thesis includes the study of several research projects which propose mobile social networks by combining existing mobile communication with the wireless connectivity functionality of mobile devices. Functionality of mobile social networks and the privacy aspects of the technology, such as LBS, direct wireless communication, RFID, etc. Legal aspects were considered. Recommendations and privacy threats list according to ENISA are presented. Finally, the background studies cover such technology as mobile telecommunication standard GBA which is the protocol on which the SWiN project design is built on. In addition, two device pairing protocols MANA and ViDPSec for mutual device authentication over a visual channel which are used by the project are studied.

The thesis work gives a detailed evaluation of the the initial SWiN secure identification design [SIC], [Naw11]. Special focus on privacy aspects of the design and particularly on identity management is given during the evaluation. Particularly the procedures of user registration, authentication, group membership acquisition, and group invitation, are examined and analyzed step by step. The following direction of the thesis work is identified as protection of user identity privacy and is formulated in a problem statement as a separate chapter of this work.

The proposal for design modifications and changes is based on introducing user and group pseudonyms to replace real identities. Two levels of pseudonyms are considered: mobile subscriber pseudonyms at the level of mobile carrier and local pseudonyms used within the mobile social network. The global pseudonym is linked with his local pseudonym achieving the fact that only the trusted mobile operator can retrieve the real identity of a user upon a special request. The MSNP remains untrusted and has no knowledge except the pseudonyms. Users prior communication must exchange the information about their identities. Thus, only friends are able to links pseudonyms with real names. As a result, the modified procedures of registration, group creation and group invitation are presented. In addition, a pseudonym generation algorithm is proposed.

The final evaluation of the design is presented in the Chapter 7. The evaluation provides a summary of the introduced changes and gives a short comparison of two versions of the modified design.

8.2 Future work

First of all, to evaluate the feasibility of the proposed modifications one could implement and realize them in a real prototype system. Also, the proposed privacy enhancements imply that the system becomes quite complex, so one would like to study the usability aspects of the proposed approach. Some other directions for the future work in the context of privacy protection within the SWiN project are:

1. The study of user and group pseudonym renewal procedures including scenarios of transition states.

2. The study of group key renewal procedures and the problem of backward and forward confidentiality.

3. The study of cases in which social groups have several moderators.

4. The representation of membership assertions as SAML assertions.

Bibliography

[3GP04] 3GPP. Transfer of application-specific user profiles in GAA. TSG SA WG3 meeting discussion document, 3rd Generation Partnership Project (3GPP), July 2004.

[3GP07] 3GPP. 3G Security; Generic Authentication Architecture (GAA); System Description. TR 33.919, 3rd Generation Partnership Project (3GPP), March 2007.

[3GP08] 3GPP. 3G security; Security architecture. TS 33.102, 3rd Generation Partnership Project (3GPP), June 2008.

[3GP10a] 3GPP. Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture. TS 33.220, 3rd Generation Partnership Project (3GPP), June 2010.

[3GP10b] 3GPP. Generic Authentication Architecture (GAA); Support for Subscriber Certificates. TS 33.221, 3rd Generation Partnership Project (3GPP), July 2010.

[3GP11] 3GPP. Numbering, addressing and identification. TS 23.003, 3rd Generation Partnership Project (3GPP), June 2011.

[BD09] S. Buchegger and A. Datta. A Case for P2P Infrastructure for Social Networks - Opportunities and Challenges. In *Proceedings of WONS 2009, The Sixth International Conference on Wireless On-demand Network Systems and Services*, Snowbird, Utah, USA, February 2009.

[BE10] D.M. Boyd and N.B. Ellison. Social Network Sites: Definition, History, and Scholarship. *Engineering Management Review, IEEE*, 38(3):16 – 31, 2010.

[BGA+08] A. Beach, M. Gartrell, S. Akkala, J. Elston, J. Kelley, K. Nishimoto, B. Ray, S. Razgulin, K. Sundaresan, B. Surendar, M. Terada, and R. Han. WhozThat? Evolving an ecosystem for context-aware mobile social networks. *Network, IEEE*, 22(4):50–55, July 2008.

[BGH09] A. Beach, M. Gartrell, and R. Han. Solutions to security and privacy issues in mobile social networking. In *Proceedings of the 2009 International Conference on Computational Science and Engineering - Volume 04*, pages 1036–1042, Washington, DC, USA, 2009. IEEE Computer Society.

[Bis04] M. Bishop. *Introduction to Computer Security.* Addison-Wesley Professional, 2004.

[BP09] J. Bonneau and S. Preibusch. The Privacy Jungle: On the Market for Data Protection in Social Networks. In *The Eighth Workshop on the Economics of Information Security (WEIS 2009)*, 2009.

[BSVD09] S. Buchegger, D. Schiöberg, L. H. Vu, and A. Datta. PeerSoN: P2P Social Networking - Early Experiences and Insights. In *Proceedings of the Second ACM Workshop on Social Network Systems Social Network Systems 2009, co-located with Eurosys 2009*, Nürnberg, Germany, March 2009.

[Bum11] Bump. http://bu.mp/, 2011.

[BWNH+06] S. Blake-Wilson, M. Nystrom, D. Hopwood, J. Mikkelsen, and T. Wright. Transport Layer Security (TLS) Extensions. RFC 4366 (Proposed Standard), April 2006. Obsoleted by RFCs 5246, 6066, updated by RFC 5746.

[CB95] D. A. Cooper and K. P. Birman. Preserving privacy in a network of mobile computers. In *Proceedings of the 1995 IEEE Symposium on Security and Privacy*, SP '95, pages 26–, Washington, DC, USA, 1995. IEEE Computer Society.

[CDFH+11] C. Castelluccia, P. Druschel, S. Fischer Hübner, A. Pasic, B. Preneel, and H. Tschofenig. Privacy, Accountability and Trust - Challenges and Opportunities. Technical report, ENISA, February 2011.

[CH06] S. Capkun and J.-P. Hubaux. Secure positioning in wireless networks. *IEEE Journal on Selected Areas in Communications*, pages 221–232, 2006.

[CKPM05] S. Cantor, J. Kemp, R. Philpott, and E. Maler. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) v2.0. Standard, Organization for the Advancement of Structured Information Standards (OASIS), March 2005. http://www.oasis-open.org.

[CM07] C.-Y. Chow and M.F. Mokbel. Enabling private continuous queries for revealed user locations. In *Proceedings of the 10th international conference on Advances in spatial and temporal databases*, SSTD'07, pages 258–273, Berlin, Heidelberg, 2007. Springer-Verlag.

[CMS10] L.A. Cutillo, R. Molva, and T. Strufe. On the Security and Feasibility of Safebook : a Distributed privacy-preserving online social network. In *PrimeLife/IFIP Summer School 2010, 6th International Summer School, IFIP AICT 320, Privacy and Identity Management for Life, August 2-6, 2010, Helsingborg, Sweden*, August 2010.

[Cro06] D. Crockford. The application/json Media Type for JavaScript Object Notation (JSON). RFC 4627 (Informational), July 2006.

[CSF+08] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280 (Proposed Standard), May 2008.

[DO10] B. van Delft and M. Oostdijk. A Security Analysis of OpenID. In Elisabeth de Leeuw, Simone Fischer-Hübner, and Lothar Fritsch, editors, *Policies and Research in Identity Management*, volume 343 of *IFIP Advances in Information and Communication Technology*, pages 73–84. Springer Boston, 2010.

[EP05] N. Eagle and A. Pentland. Social serendipity: mobilizing social software. *Pervasive Computing, IEEE*, 4(2):28 – 34, 2005.

[Fac11] Facebook. http://www.facebook.com/, 2011.

[FH02] S. Farrell and R. Housley. An Internet Attribute Certificate Profile for Authorization. RFC 3281 (Proposed Standard), 2002.

[FHBH+99] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, and L. Stewart. HTTP Authentication: Basic and Digest Access Authentication. RFC 2617 (Draft Standard), June 1999.

[Fou11] Foursquare. http://foursquare.com/, 2011.

[GG03] M. Gruteser and D. Grunwald. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In *Proceedings of the 1st international conference on Mobile systems, applications and services*, MobiSys '03, pages 31–42, New York, NY, USA, 2003. ACM.

[GMN04] C. Gehrmann, C. Mitchell, and K. Nyberg. Manual authentication for wireless devices. *RSA Cryptobytes*, January 2004.

[Gow11] Gowalla. http://gowalla.com/, 2011.

[GTF08] S. Guha, K. Tang, and P. Francis. NOYB: privacy in online social networks. In *WOSP '08: Proceedings of the first workshop on Online social networks*, pages 49–54, New York, NY, USA, 2008. ACM.

[GyP11] GyPSii. http://www.gypsii.com/, 2011.

[HP00] J. Schaad H. Prafullchandra. Diffie-Hellman Proof-of-Possession Algorithms. RFC 2875 (Proposed Standard), 2000.

[Hum07] L. Humphreys. Mobile Social Networks and Social Practice: A Case Study of Dodgeball. *Journal of Computer-Mediated Communication*, 13(1), 2007.

[KBC97] H. Krawczyk, M. Bellare, and R. Canetti. Hmac: Keyed-hashing for message authentication. RFC 2104 (Proposed Standard), 1997.

[KSK03] M.O. Koutarou, K. Suzuki, and S. Kinoshita. Cryptographic Approach to "Privacy-Friendly" Tags. In *In RFID Privacy Workshop*, 2003.

[Kum10] P. Kumari. Requirements analysis for privacy in social networks. *Proc. 8th Intl. Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods (VG)*, October 2010.

[KW08] B. Krishnamurthy and C.E. Wills. Characterizing privacy in online social networks. In *Proceedings of the first workshop on Online social networks*, WOSP '08, pages 37–42, New York, NY, USA, 2008. ACM.

[Lab] RSA Laboratories. Pkcs 11: Cryptographic token interface standard. http://www.rsa.com/. Latest visit September 2011.

[LGA+05] P. Laitinen, P. Ginzboorg, N. Asokan, S. Holtmanns, and V. Niemi. Extending cellular authentication as a service. In *Commercialising Technology and Innovation, 2005. The First IEE International Conference on (Ref. No. 2005/11044)*, 2005.

[MW04] D. Molnar and D. Wagner. Privacy and security in library RFID: issues, practices, and architectures. In *Proceedings of the 11th ACM conference on Computer and communications security*, CCS '04, pages 210–219, New York, NY, USA, 2004. ACM.

[Nat] United Nations. The universal declaration of human rights. http://www.un.org/en/documents/udhr/. Latest visit September 2011.

[NAT02] A. Niemi, J. Arkko, and V. Torvinen. Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA). RFC 3310, Internet Engineering Task Force, September 2002.

[Naw11] O. Nawaz. Secure identification in social wireless networks. Diploma thesis, Blekinge Institute of Technology, 2011.

[OJ08] H.-K. Oh and S.-H. Jin. The Security Limitations of SSO in OpenID. In *Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on*, volume 3, pages 1608 –1611, 2008.

[Olk06] T. Olkkonen. Generic authentication architecture. Security and Privacy in Pervasive. Computing, Seminar on Network Security, 2006.

[Ope] OpenID. Specifications. http://openid.net/developers/specs/.

[PK01] A. Pfitzmann and M. Köhntopp. Anonymity, unobservability, and pseudeonymity - A proposal for terminology. In *International workshop on Designing privacy enhancing technologies: design issues in anonymity and unobservability*, pages 1–9, New York, NY, USA, 2001. Springer-Verlag New York, Inc.

[PPW+09] S. Park, H. Park, Y. Won, J. Lee, and S. Kent. Traceable Anonymous Certificate. RFC 5636 (Experimental), 2009.

[PrB+10] M. Papadopouli, A. Årnes, J.A. Bombin, E. Boschi, S. Buchegger, R.B. Cortiñas, F. Gaudino, G. Hogben, T. Karagiannis, C. Manifavas, K. Mitrokotsa, N. Nikiforakis, P. Papadimitratos, G. Roussos, and K. Tsakona. Mobile Identity Management. Technical report, ENISA Position Paper, April 2010.

[Ros07] D. Rosenblum. What Anyone Can Know: The Privacy Risks of Social Networking Sites. *IEEE Security and Privacy*, 5:40–49, 2007.

[Sei05] C. Seidler. RFID Opportunities for mobile telecommunication services. http://www.itu.int/ITU-T/techwatch/rfid.pdf, 2005.

[SGSZ] M. Salzberg, D. Grippi, R. Sofaer, and I. Zhitomirskiy. Decentralize the web with Diaspora - Kickstarter. http://www.kickstarter.com/projects/196017994/diaspora-the-personally-controlled-do-it-all-distr/. Latest visit September 2011.

[SIC] SICS. Social Wireless Network Secure Identification, Project page. http://www.sics.se/projects/swin/. Latest visit September 2011.

[SKS10] P. Sovis, F. Kohlar, and J. Schwenk. Security Analysis of OpenID. In *Sicherheit*, pages 329–340, 2010.

[SO11] L. Seitz and O. Ohlsson. System Architecture and Secure Identity Management Design (D2,D3), SWiN Project, 2011.

[Str07] D. Strobel. IMSI Catcher, 2007.

[Tim] The New York Times. Where Are You? Show Them With Google Latitude. http://bits.blogs.nytimes.com/2009/02/04/where-are-you-show-em-with-google-latitude/. Latest visit September 2011.

[Twi11] Twitter. http://www.twitter.com/, 2011.

[VMG+01] K. Virrantaus, J. Markkula, A. Garmash, V. Terziyan, J. Veijalainen, A. Katanosov, and H. Tirri. Developing gis-supported location-based services. In *Web Information Systems Engineering, 2001. Proceedings of the Second International Conference on*, volume 2, pages 66 –75 vol.2, December 2001.

[weba] Facebook Privacy Controls. http://www.facebook.com/privacy/explanation.php. Latest visit September 2011.

[webb] Facebook statistics. http://www.facebook.com/press/info.php?statistics. Latest visit September 2011.

[WF08] S. Wynn and D. G. Fraser. US Patent 2008/0195741, System and method for enabling wireless social networking, 2008.

[Wik] The Official Diaspora Wiki. https://github.com/diaspora/diaspora/wiki. Latest visit September 2011.

[WSRE03] S. Weis, S. Sarma, R. Rivest, and D. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. March 2003.

[ZDN11] ZDNet. Facebook and Google must follow EU privacy rules. http://www.zdnet.co.uk/news/regulation/2011/03/17/facebook-and-google-must-follow-eu-privacy-rules-40092179/, March 2011.

[ZKT] D. Zisiadis, S. Kopsidas, and L. Tassiulas. ViDPSec visual device pairing security protocol.

[ZSZF10] C. Zhang, J. Sun, X. Zhu, and Y. Fang. Privacy and security for online social networks: challenges and opportunities. *Network, IEEE*, 24(4):13–18, 2010.

Appendix A

Invitation vector in SAML format (Example)

```
<Assertion ID="_33776a319493ad607b7ab3e689482e45"
  IssueInstant="2011-07-17T20:31:41Z">
   <Issuer>Alice</Issuer>
   <Signature>...</Signature>
   <Subject>
      <NameID>Bob</NameID>
      <SubjectConfirmation
         Method="urn:oasis:names:tc:2.0:cm:holder-of-key">
         <SubjectConfirmationData>
            <ds:KeyInfo>
               <ds:X509Data>
                  <ds:X509Certificate>
MIICiDCCAXACCQDE+eiWrm62jANBgkqhkiG9w0BAQQFADBFMQswCQYDVQQGEwJ
UzESMBAGA1UEChMJTkNTQS1URVNUMQ0wCwYDVQQLEwRVc2VyMRMwEQYDVQQDEw
pTUC1ZXJ2aWNlMB4XDTA2MDcxNzIwMjE0MVoXDTA2MDcxODIwMjE0MVowSzELM
AkGA1UEBhMCVVMxEjAQBgNVBAoTCU5DU0EtVEVTVDENMAsGA1UECxMEVXNlcjE
ZMBcGA1UEAwwQdHJzY2F2b0B1aXVjLmVkdTCBnzANBgkqhkiG9w0BAQEFAAOBj
QAwgYkCYEAv9QMe4lRl3XbWPcflbCjGK9gty6zBJmp+tsaJINM0VaBaZ3t+tSX
knelYifenCc2O3yaX76aq53QMXy+wKQYe8Rzdw28Nv3a73wfjXJXoUhGkvERcs
cs9EfIWcCg2bHOg8uSh+Fbv3lHih4lBJ5MCS2buJfsR7dlr/xsadU2RcCAwEAA
TANBgkqhkiG9w0BAQQFAAOCAQEAdyIcMTob7TVkelfJ7I1j0LO24UlKvbLzd2O
PvcFTCv6fVHxEjk0QxaZXJhreZ6rIdiMXrEzlRdJEsNMxtDW8sVp6avoB5EX1y
3ez+CEAIL4gcjvKZUR4dMryWshWIBHKFFul+r7urUgvWI12KbMeE9KP+kiiiiT
skLcKgFzngw1JelmHhTcTCrcDocn5yO2d3dog52vSOtVFDBsBuvDixO2hv679J
R6Hlqjtk4GExpE9iVI0wdPE038uQIJJTXlhsMMLvUGVh/c0ReJBn92Vj4dI/yy
6PtY/8ncYLYNkjgoVN0J/ymOktn9lTlFyTiuY4OuJsZRO1+zWLy9g==
                  </ds:X509Certificate>
               </ds:X509Data>
```

```
          </ds:KeyInfo>
        </SubjectConfirmationData>
      </SubjectConfirmation>
    </Subject>
    <Conditions
      NotBefore="2011-07-17T23:26:31Z"
      NotOnOrAfter="2011-07-18T23:26:31Z">
    </Conditions>
    <AttributeStatement>
      <Attribute Name="groupRole:SWiN">
        <AttributeValue>temporaryMember</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
```

Appendix B

Social certificate in SAML format (Example)

```
<Assertion ID="_33776a319493ad607b7ab3e689482e45"
  IssueInstant="2011-07-17T20:31:41Z">
   <Issuer>MSNP</Issuer>
   <Signature>...</Signature>
   <Subject>
      <NameID>Alice</NameID>
      <SubjectConfirmation
         Method="urn:oasis:names:tc:2.0:cm:holder-of-key">
         <SubjectConfirmationData>
            <ds:KeyInfo>
               <ds:X509Data>
                  <ds:X509Certificate>
MIICiDCCAXACCQDE+eiWrm62jANBgkqhkiG9w0BAQQFADBFMQswCQYDVQQGEwJ
UzESMBAGA1UEChMJTkNTQS1URVNUMQ0wCwYDVQQLEwRVc2VyMRMwEQYDVQQDEw
pTUC1TZXJ2aWNlMB4XDTA2MDcxNzIwMjE0MVoXDTA2MDcxODIwMjE0MVowSzEL
MAkGA1UEBhMCVVMxEjAQBgNVBAoTCU5DU0EtVEVTVDENMAsGA1UECxMEVXNlcj
EZMBcG1UEAwwQdHJzY2F2b0B1aXVjLmVkdTCBnzANBgkqhkiG9w0BAQEFAAOBj
QAwgYkCgYEAv9QMe4lRl3XbWPcflbCjGK9gty6zBJmp+tsaJINM0VaBaZ3t+tS
XknelYifeCc2O3yaX76aq53QMXy+wKQYe8Rzdw28Nv3a73wfjXJXoUhGkvERcs
cs9EfIWcCg2bHOg8uSh+Fbv3lHih4lBJ5MCS2buJfsR7dlr/xsadU2RcCAwEAA
TANBgkqhkiG9w0BAQQFAAOCAQEAdyIcMTob7TVkelfJ7I1j0LO24UlKvbLzd2O
PvcFTCv6fVHxEjk0QxaZXJhreZ6rIdiMXrEzlRdJEsNMxtDW8sVp6avoB5EX1y
3ez+CEAIL4gcjvKZUR4dMryWshWIBHKFFul+r7urUgvWI12KbMeE9KP+kiiiiT
skLcKgFzngw1JselmHhTcTCrcDocn5yO2d3dog52vSOtVFDBsBuvDixO2hv679
JR6Hlqjtk4GExpE9iVI0wdPE038uQIJJTXlhsMMLvUGVh/c0ReJBn92Vj4dI/y
y6PtY/8ncYLYNkjgoVN0J/ymOktn9lTlFyTiuY4OuJsZRO1+zWLy9g==
                  </ds:X509Certificate>
               </ds:X509Data>
```

```
          </ds:KeyInfo>
        </SubjectConfirmationData>
      </SubjectConfirmation>
    </Subject>
    <Conditions
          NotBefore="2011-07-17T20:15:27Z"
          NotOnOrAfter="2011-07-24T20:15:27Z">
    </Conditions>
    <AttributeStatement>
      <Attribute Name="groupRole:SWiN">
        <AttributeValue>Moderator</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
```