MASTER THESIS

Identity Management approach in Internet of Things

Aalborg University

2015

Master Thesis

Identity Management Approach in Internet of Things

Supervisor: Ass. Prof. Albena Mihovska **Student: Vanya Zdravkova**

Co-supervisor: PhD. Bayu Anggorajati

06.2015

Aalborg

Contents

List of Figures

List of Tables

List of Abbreviations

3GPP	3rd Generation Partnership Project
AAL	Ambient Assistant Living
ABAC	Attribute-Based Access Control
ACL	Access Control List
ACM	Access Control Matrix
AmI	Ambient Intelligence
API	Application Programming Interface
App-ID	Application Identifier
AS	Authorization Server
CDP	Computing Device Part
CDR	Computing Device Recognition
CN	Core Network
CONN-ID	Connection Identifier
DS	Device Subsystem
EPC	Electronic Product Code
ETSI	European Telecommunications Standards Institute
gloInt	global ownership/interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information communication technologies
ID	Identifier
IdM	Identity Management
IDSS	Intelligent Decision Support Systems
IdP	Identity Provider
IdPS	Identity Provider Subsystem
IdPSP	Identity Provider Subsystem Part
IoP	Internet of People
IoT	Internet of Things
IR	Infra-Red
JSON	JavaScript Object Notation
locInt	Local ownership/interface
M2M	Machine To Machine
MAGNET	My personal adaptive global network
MAS-ID	MAS Identifier
M-Bus	Meter-Bus
MSBF-ID	MSBF Identifier
MSMP	MAGNET Service Management Platform
NFC	Near Field Communication
Node-ID	Node Identifier

Non-userIntDP	Non-user Interface Device Part
OASIS	Organization for the Advancement of Structured Information Standards
OID	Object Identifier
OIdP	OpenID Identity Provider
ONS	Object Name System
OP	OpenID Provider
PAN	Personal Area Network
PIP	Personal Identity Provider
PN	Personal Network
PROV-ID	Provider Identifier
RBAC	Role-Based Access Control
RFID	Radio Frequency Identifier
RO	Resource Owner
RS	Resource Server
SAML	Security Assertion Markup Language
SCL	Service Capabilities Layer
SCL - ID	Service Capabilities Layer Identifier
SoA	State-Of-the-Art
SP	Service Providers
SS	Service Subsystem
SSh	Smart Sheet
SSP	Service Subsystem Part
STSO	Single Thing Sign On
TLS	Transport Layer Security
TSP	Thing Subsystem Part
UA	User Agent
UML	Universal Modeling Language
unidevID	unique device ID
unidomID	unique domain ID
uniuID	unique user ID
UP	User as a Part
UPID	User-Provided Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTRAN	Universal Terrestrial Radio Access Network
WiMAX	Worldwide Interoperability for Microwave Access
W-LAN	Wireless Local Area Network
WSN	Wireless Sensor Networks
xDSL	x Digital Subscriber Line
XML	Extensible Markup Language

Abstract

Nowadays, 'people are united in their need to be connected to the Internet anywhere, anyhow, anytime. Thanks to the evolution of Information communication technologies (ICT) more and more exclusive services (smart homes, telemedicine, e-Health applications etc.) are available for the users through heterogeneous Internet of Things (IoT) networks, driven by machine to machine (M2M) communication.

Although, the communication is established primarily by using devices, the human users are real “generators” and “consumers” of the input and output information. Thus, the human user has to be considered as a “smart” IoT object, thus he/she should be identified, authenticated, authorized.

The process of user identification is considered to be very delicate due to the concerns for the people′s willingness of sharing private information and data. At the same time, the utilized by a certain user devices, should be taken into consideration. Within this context there is a need of attractive user identification and Identity Management (IdM) mechanisms, involving all of the objects in IoT. Furthermore, the active role of the user in the creation of the rules of identification, and having always responsive services, are extremely important and slightly moving the focus to the concept of ′Internet of People′.

The present master thesis addresses the problems of user identification and proposes the design of a novel Single Thing Sign On (STSO) IdM system where the end-user is in the middle of a user-centered services ecosystem. The proposed scheme enables user recognition and assigned services access only by identification of one of the “things” related to the user (personal computing devices, sensors etc). Besides, the author proposes a novel user identification method driven by computing device recognition algorithm (CDR algorithm).

The proposed CDR algorithm and IdM system were evaluated through a set of technical and business analytical methodologies in order to proof the concept. The discussion confirms the importance of the researched matter and further clarifies the objectives.

Keywords: *IoT, M2M, user identification, authentication, IdM, user-centered*

Chapter 1

Introduction

The goal of this chapter is to identify the problem and explain the motivation for solving it in context of Identity Management (IdM) in Internet of Things (IoT). The goals and objectives of the thesis research are clarified. The research workflows, methodology of the thesis and out of the scope issues are presented.

1. Introduction

The Internet presents a unique interconnected system which enables devices to communicate globally using set of standard protocols and connecting various heterogeneous networks - academical, business, governments etc. In the first years, the Internet was represented by static web sites and email communication. Nowadays, different forms of Internet implementation could be seen everywhere around us, part of many different aspects of our lives providing plenty of services and applications, and trying to meet each user's needs no matter time and place. The main "secret" is hidden behind the digitalization of the user and all of the user-friendly and automated mechanisms.

The demand of using internet technologies reflects respectively into all of the users' devices in one way or another, and they have become mobile and closer to the users than ever. Today, the presence of smart devices providing connectivity to the world at each second is considered as mandatory part of our life. Thus, the number of connected devices rapidly increases each year. That requires an autonomous device communication to be created. One of the promising solutions today is known as the Internet of things (IoT). IoT is an informational network that allows the look-up of information about real-world objects interact directly with each other by means of a unique identifier (ID) [1].

As an important part the "communication" has to be considered and also the collaboration between all of those different devices through the Internet and based on the advances of wireless access technologies, formed by machine to machine (M2M) communication [2].

The result of such kind of M2M communication is information, which on one hand is related to the people and, on the other hand, is produced by them. Furthermore, the data ownership is a key aspect, thus, the establishing of secured communication, accessing the resources, and the user identification and authentication are crucial and play an important role because the "actual users" are humans [3].

The development of the Information Communication Technology (ICT) provides the various methods for user identification and attractive Identity Management (IdM) mechanisms such as

Single Sign On (SSO) whereby the user effort of remembering passwords is simplified on web level.

As a central part of the IoT ecosystem, the users can be considered as different “smart” objects being part of creating, gathering and managing information by personal and/or shared devices, and can be identified in the IoT in the same manner as the other objects (sensors or actuators).

One of the most important role and contribution in the IoT is awarded to the users and their personal smart devices. That is an opportunity and a novel ways for the people to interact and participate actively worldwide within the IoT. Thus, it is a solid basis in the process of making smart and sustainable surroundings a reality [4].

As an active players in IoT, the users impact into existing ubiquitous internet, new ways of making electronics and creating more suitable personal-oriented human interfaces. That all is a solid fundamental to think about enabling the Internet of People (IoP) which is encompassed internet-enabled personal electronics, serves “the human needs from medical to entertainment” [5].

Looking into the latest technologies and taking into consideration the future perspective for the Internet development, the user will take a central part. Therefore, the user identification is crucial and will be attractive field for research and finding more and more user-friendly, time- and effort- saving solutions and IdM systems.

1.1. Problem statement

From a technical point of view, the IoT presents network of uncountable number of global connected objects - devices, sensors or actuators, providing different services over the Internet. As a consequence for the business, IoT means a plethora of new opportunities, new fields for implementation of devices, disruptive business use cases, resulting to scenarios and services for the end-users.

The usage of multiple topologies and different protocols for communication between devices and sensors in IoT and the fact that there is no common solution, rise up the need for identity management, as a common technology to provide successful communication framework for the objects in IoT [6]. Referring to all the various solutions, the enabling of user identification and authentication depends on the network layout and all sets of rules and capabilities integrated in the certain network [7].

Depending on the specific scenarios, objects may require to be uniquely identified or to be identified as belonging to a given class (e.g., this object is a pen, regardless of which pen it is). Each object should be identifiable. Identity managements needs the best object identification for its purposes, no matter the type of technologies being used to serve the given service or application to the end-user [8]. The access to connected shared devices will enable gathering contextual metadata and sensors data and will enable user centered responsive services. To addresses the problems stated in the section, an novel IdM system which will aim to identify end-user and at the same time provide user-centered services to him/her by identifying things in IoT such as personal computing devices, sensors etc. is proposed, The enabling IdM feature is introduced by the author as Single Thing Sign On (STSO).

The scope of the conducted research is limited to M2M and IoT and in particular focuses on the IdM whereby all of the things part of IoT such as human users, computing devices and non-user interface devices (sensors, actuators) are considered. Within the scope of the thesis is to analyze and recommend a number of suitable solutions. The identification and authentication processes as well as related to the IdM identifier fall within the scope.

1.2. Motivation and goals

The motivation for conducting the research in the area of IdM in IoT is the lack of sustainable and flexible solutions which to address some of the main enablers of the technology. Some early solutions are now being implemented but they still need improvement and standardization [6]. The full potential of IoT means going beyond the enterprise centric systems and moving towards a user inclusive IoT, in which IoT devices and contributed information flows provided by people are encouraged [4]. This will allow new user-centric IoT information flows and new generation of services of high value for the society.

1.2.1. Identification and Authentication

The end-user identification can be performed via various tools, devices, network equipment or protocols but currently there is no common solution. The user identification and authentication is crucial for the IoT in order to isolate threats and enable policy enforcement for different users or groups. The option to identify and/or authenticate the user is dependent on the network layout, the security rules that are used in the network and the capability to integrate with an external password server [7].

1.2.2. Identity Management

Managing increasing number of devices requires scalable and efficient authentication, access control and, Identity Management (IdM) mechanism. In his work Mahalle [9] recognizes the problem as “This broader scope of interactions enhances the need to extend current IdM models to include new hierarchical identifiers, and addressing based on clustering, trust, and capability-based access control, and mutual authentication schemes. Pervasive IoT objects are equipped with the devices with communication and computation capability with resource constraints”. The proposed IdM system addresses identity management related to the certain user by involving the entire information about users’ credential, utilized computing devices, and personal or public non-user interface devices.

1.2.3. Mobility of Devices

Another important aspect that should be taken into consideration for designing IdM in IoT is the mobility of the devices, the dynamic topologies, and the ad-hoc nature. There are many existing solutions for IdM [10] [11], with identities that are used by the end users and services to identify themselves in the networked world. In the proposed IdM, the mobility of the devices will be considered as an action whereby the user changes his/her location, respectively devices and the proposed here IdM functionalities will continuously provide all of the identified services to the user, no matter time and place.

1.2.4. Responsive Services

From a user perspective, the IoT will enable a large number of new user centered and responsive services, which will need to answer the users’ needs and support them in everyday activities. The

IoT will trigger the shift from the current vision of “always on service” , typical for the Web, to “always-responsive” situated services, built and composed at run-time to respond to a specific need and able to account for the user’s context [8]. In order to meet that requirement, the proposed here IdM system will aim to satisfy the user’s needs by specific context-aware user centered applications and services, based on users’ profiles, combined with mobility of the devices and identity management features.

1.3. Objectives

The following research objectives were identified:

- Study various user- and device- oriented IdM systems and frameworks in heterogeneous IoT scenarios and obtain a reference state-of-the-art (SoA) status of the technology;
- Identify potential requirements from user and system perspectives how to improve the SoA in terms of IdM;
- Define a particular user scenario for implementation of IdM framework;
- Design a novel user-centered IdM system in IoT scenario, supporting the complexity communication;
- Define communication relationships in the proposed IdM
- Propose a novel identification algorithm for supporting automated user identification;
- Evaluate and analyze the system’s technical and business aspects
- Discuss and find out system’s weaknesses, if there are any.

1.4. Delimitation

This section discusses the aspects which are not investigated due to they are out of the scope of the thesis.

- The detailed process for the software artefacts development and implementation
- The data flow procedures for the identification
- The process of providing the users’credentials to the device
- The information regarding the specific data format
- User full-provisioning identification and verification process
- The access rules
- The thing profile setup

1.5. Methodology

The main focus falls on designing a novel IdM system which involves the 'things' in IoT (human user and different devices such as computing and smart devices, sensors, actuators etc.) and expresses the communication between them. The system is analyzed from business and technical perspectives in relation to the identified user and system requirements..

The first step is to make a theoretical analysis of various IdM and communication systems proposed for M2M and IoT heterogeneous networks. Based on that analysis, we derive the user and system requirements. An use-case scenario is defined to describe how the system is applicable in a real-life situation. Then, a novel user-centered IdM system architecture is proposed. The system communication flows are explained by an UML diagram and a class-diagram scheme. The general STSO connection and authentication procedures are given by UML sequence diagrams. The analysis of the system takes into consideration both the technical and the business aspects. From a technical perspective, the proposed IdM is evaluated with comparative analysis applied on existing solutions, predefined user and system's requirements and the system implementation. Concerning the business aspect, strategies and disruptiveness of the proposed IdM are assessed.

1.6. Novelty and contribution

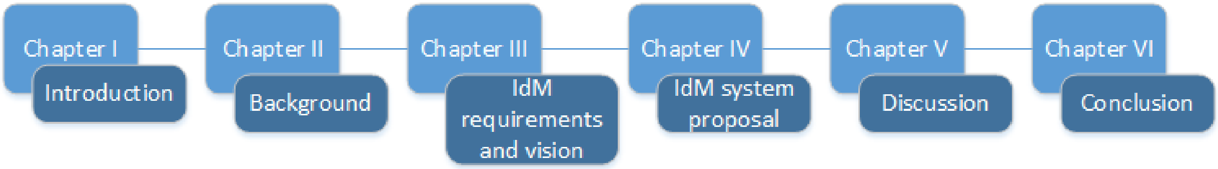
The goal of the thesis is to research IdM solutions proposed for IoT and to design and develop a novel identity management solution. The main novel contributions of this research project are as follows:

- An algorithm for user identification based on computer-device recognition
- A coefficient for the identification rate of the computing device
- An identifier format
- An identification process involving all of the things in IoT – STSO feature
- A conceptual system for IdM

1.7. Thesis Outline

A chapter content overview of the thesis is given in Table 1.1.

Table 1.1 Chapter content overview of the thesis



Chapter II describes the identification, authentication and authorization processes. The use of identification is demonstrated by reference use-case scenarios. An algorithm for user identification and coefficient for assessment of the algorithm are proposed.

Chapter III includes information about the IoT heterogeneous networks and identification schemes. The research challenges are identified. This chapter introduces the identifier format which will be used in the proposed IdM system.

Chapter IV defines the IdM requirements considering the user's and system's perspectives for IdM in IoT based on existing identity management solutions. The vision of IdM is presented as well. This chapter proposes a concept for an IdM system that addresses the identities management of "things" in IoT heterogeneous networks. As advantages, the system proposes and automated identification and enables responsive services. The schematic overview and communication information flow of the system, general STSO connection and authentication are presented by Universal Modeling Language (UML) diagrams.

Chapter V presents conclusion as a summary of the contributions to this thesis research, and discusses the future perspectives and open issues which can be explored and further investigated.

Chapter 2

User identification

This chapter introduces a brief IoT overview based on a literature research. The importance of identification, authentication and authorization processes is presented. A use-case is given in order to illustrate a real-life scenario for using identity of things. Based on the conducted research, an algorithm for user identification is proposed. Coefficient which defines the identification rate of computing device is proposed and used for assessment and analysis of the algorithm.

2.1. IoT overview

Back in 1988, Weiser [12] introduced the “Ubiquitous Computing”. He suggested the following forms of ubiquitous computing devices which can provide services to the end user regardless of time or location: tab, pads, and boards. Since then, a lot has changed in terms of computational power and integrity of the computing devices as today they may be found in almost every “thing” around us, being interconnected and capable of exchanging data.

Moving the focus towards today [13], IoT is “ubiquitous concept where physical objects are connected over the Internet and are provided with unique identifiers to enable their self-identification to other devices and the ability to continuously generate data and transmit it over a network”. Hence, the security of the network, data and sensor devices is a paramount concern in the IoT network as it grows very fast in terms of exchanged data and interconnected sensor nodes.

Alongside with the increasing number of network services and applications which constantly provide different types of information, the opportunity of the user to interact with the “things” and “objects” increases constantly and that trend is predicted to continue [14]. The things in IoT may refer to a myriad of connected devices, objects or sub networks for example sensors and actuators connected over Zigbee, Bluethoot, etc.

The architecture supporting interconnected devices evolve further and find implementations in areas like logistics, farming, industry, home automation and many others are already a fact but the restrictions in terms of interconnection solutions from different vendors, communities and standard groups become more obvious. Referring to the business aspects, the IoT enables a plethora of new opportunities, disruptive business models and use case scenarios. In many cases those connected devices and objects are not Hypertext Transfer Protocol (HTTP) driven and that is why there is a lack of decent application integration layers and the applications development is hard to be achieved.

Being more focused on the issues in IoT, the next logical step toward the ubiquitous deployment of applications is the building on top of the already widely used Web technologies. Concerning the importance IoT related open issues, the IdM is recognized as one of the main enablers of the technology. A lot of research has been conducted [15] [9], but there is no overall framework for identity recognition and management across different solutions [6].

The high level overview of the IoT is illustrated in Figure 2.1. It consists of cauterized infrastructure of sensors, exchanged routing data between the nodes, which nodes might be used as gateways in the sub-network of sensors [9].

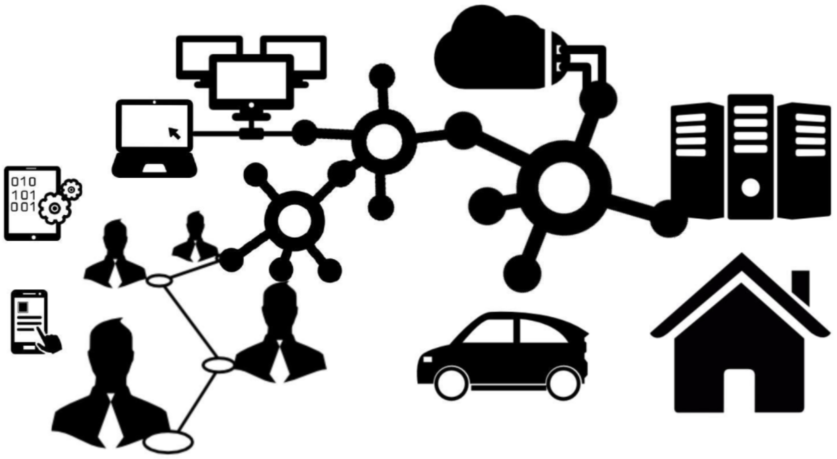


Figure 2.1 High level view of IoT [9]

The IoT vision for global network of interconnected devices and objects and their real-time communication has been prompted by the M2M paradigm. As a result of the M2M technology, plenty of applications possibilities are available in different aspects - automation processes, tracking, monitoring and control, entertainment etc [16].

Very similar to IoT, “The M2M communications is a broad term describing any technology that enables networked devices to exchange information and perform actions without manual assistance of human personnel” [17].

The M2M devices are performing specific tasks corresponding to their functionalities. These devices also act as independent network nodes, capable of communication over different types of messaging protocols as well as responding to incoming requests.

M2M communication is expected to deploy a technology in order to create intelligent applications and services that are scalable, reliable and embedded, thus the M2M term is closely related to the IoT technology. M2M and IoT are being expected to enable automation and self network management which is needed to support the large number of connected nodes. [18]

The scope of applications deployed by M2M technology is broad. Some of the areas expected to utilize M2M and IoT concern smart metering, automation, ambient assisted living applications, ambient environment or large-area automation, e-health, etc. Working in different environment and context it should be noted that the solutions for user identification and user identity management are considered to be among the enables of the technology.

2.2. Identity – background information

2.2.1. Identification

Identities are the windows through which users interact with their things and consume services in today's world. In context of IoT, this concept of identity extends to things. Identities can be considered as end points so that it is easy to ensure access to endpoint independent of thing being used [9].

The user identification process can be explained as an interaction whereby the user identity is provided to the security system. The identification provides access to and the modification of data by a certain personal, and enables services and communications to be customized [19]. In IoT context, identification can be explained as an association of attributes which represents identifiers. A unique characteristic which is associated with an entity known as an attribute, like sensor with Radio Frequency Identifier (RFID) tag. The real meaning of the identifiers is to differentiate the objects from the others, and they depend on the context [9]. Identifier, which meaning is to identify the entity in a unique way and often that is the only one purpose, is a represented of the strong identifiers. If the identifier enables sharing of its value to the other entities in the same system, then it is a weak identifier [20]. As a summary of the stated above, one common device and object identifier would be beneficial in IoT world.

All identity data is create, managed and protected by the IdM system. More information about IdM is provided in Chapter IV.

2.2.2. Authentication

A) Human user authentication

The user identity is validated by the process of authentication whereby the provided from the user evidence is verified, it is real or not, by requests for user credentials. Credentials are presented unique characteristics (RFID, Near Field Communication (NFC) tag, face or voice recognition) or information (password) by the user to the authentication parties are, and they are fundamental. Authentication credentials can be one or more and they are part of one of the following groups [19]:

- *"Something you know"* or "*something a user knows*", type of authentication is based on a shared secret between the involved parties. The typical example is a password authentication scheme [19]. Other various ways for identification already exist such as drawing patterns on smart devices screens, graphical images which have to be recognized. Those methods are unable to replace the usage of traditional password identification because of their usage and insufficient security advantage [21].
- *"Something you are"* or "*something a user is*" - here, the main role is played by the provided biometric information such as fingerprints, retina or facial scan, voice etc [19]. The weakness is that there is a risk of unintended usage of the digital biometric information and potential threat of theft or it might be copy and use to falsify certain body part because the biometrical information is unique and distinctive in corporation to the user and cannot be changed as password for instance [22].
- *"Something you have"* or "*something a user has*" - in that case, the authentication requires to be provided an actual item (tokens) where the user's secret is stored such as smart card, a Universal Serial Bus (USB) stick, a serial tap etc [19].The user does not need to remember secret as it is in the password authentication. It emphasizes a question about whether it can provide real user identification since the sharing of the items between users. In addition, those items can be stolen or lost [23].

Analyzing the user's behavior regarding browsing, mouse click or other patterns is an alternative method for identification. However, the behavior method is imitable, non-resistible to attacks and its usage is limited in secure systems [24]. Behavioral biometrics is harder to imitate because the capture may depend on a different time of the day, but it is also harder to produce correct results [25].

The validation of user identity is the main aim for the both identification and authentication processes.

B) Device authentication

Device authentication is also an important aspect in IoT because of the devices' role and broad usage everywhere around us.

- *"Something that is characteristic to a device"* are required behavioral credentials or physical context (such as geographic features or transmitted signal frequency) in order to authenticate and determine the device's identity. The mentioned credentials are more often considered as context-based than identity-based [26].
- *"Something a device has"* - here, the secret key is stored in device and has to be provided in order to prove user identification (mentioned above as *"something a user has"*). Device authentication is often used in an automatic sense/way without requiring presence of user at the certain moment. Therefore, the secret stored in devices is meaningful for device authentication also, not only for the user's [23].

2.2.3. Authorization and Accounting

Although, the process of authentication enables and verifies the user identity, if one wants to access certain resources in the system, he/she has to have the rights for performing that action. By the authorization process, the system determines whether a specific user is allowed or not to access a certain information or features [19]**.**

Referring to Rotondi [27] and Todorov [19] the procedure for authorization is performed in a policy decision point, where the security policy for a requested resource access is compared with the permissions of the authenticated entity that request it. The access control mechanisms are classified as follows:

- Access Control Lists (ACLs) - enables the subject (certain entity) to perform explicitly specified individual actions with the objects (specific resources). The access control matrix (ACM) is more generalized systematic approach which enables access rights in a matrix, consisting of subject-object pair matrix elements. The weak asset of the technique is complicated management of large number of subjects and objects.

- Role-Based Access Control (RBAC) - by introducing an additional role layer and considering the role as a subset, it is suitable for solving the mentioned above rights management problem, where the access rights are associated to roles rather the specific subjects. Each object can have one or more roles which allow it to operate to more than one access right subsets.
- Discretionary Access Control and Mandatory Access Control - the main focus is on the provider of access rights. Typically, the human is a resource owner in discretionary access control and he/she determines the access rights to his/her resources. In mandatory access control, a central administrator specifies subjects' right for accessing the objects in the system.
- Attribute-Based Access Control (ABAC) - attributes of identities, rather than identities themselves, are used as a basis for granting access control to the resources. This method does not allow specific identities detection

As a part of further increasing of the secured perspective, operations of a certain entity (often human user) are recorded. The process is called accounting and it is useful from a security aspect because it is activated no matter if authentication is successful or not and can be used as a proof for security investigations [19].

2.3. Use case

Here, a use case in the context of using thing identity in real-life scenario is defined.

The user Charlene who is 60 years old has installed several identities in her personal mobile devices (smart phone, tablet, laptop etc.) and she uses them to access different services (applications, web platforms and services, etc). Due to her age Charlene takes serious care for her health performance, and she has an installed eHealth platform in her home. The platform consists of wearable medical and motion sensors supported with ambient environment monitoring sensors. The eHealth platform offers Charlene telehealth monitoring service which to support her independent living and, when is needed, notify the respective authorized caregivers and family members to access her data in order to take right actions for her's health.

Charlene visits an activity center monthly and spends a week there. She brings her personal devices but unfortunately she cannot take the home sensors. She, as well, uses some of the shared equipment in the center. When Charlene wants to access the local Wi-Fi network, in a classical situation, she would ask for the private Wi-Fi password of the activity center. Then, she should type it on each device which she would like to utilize. Additionally, she should activate multiple services supporting her ambient assisted living. Conversely, in our case, all of her identities are stored in a web cloud (where the password for the Wi-Fi network in activity center is also stored) and she can easily use them after her identity validation. Typically, that validation requires retyping of a username and a password. Fortunately, Charlene is using intelligent IdM system that offers automatic user identification based on finding her mobile devices. She Charlene logs in automatically and all of her devices gain access to the Wi-Fi network seamlessly. Behind that process, the IdM automatically activates the assigned to her services and enables collecting information from them in personalized meaningful manner to her. Thus, the system provides responsive services no matter time and place to her. The use-case diagram is presented in Figure 2.2.

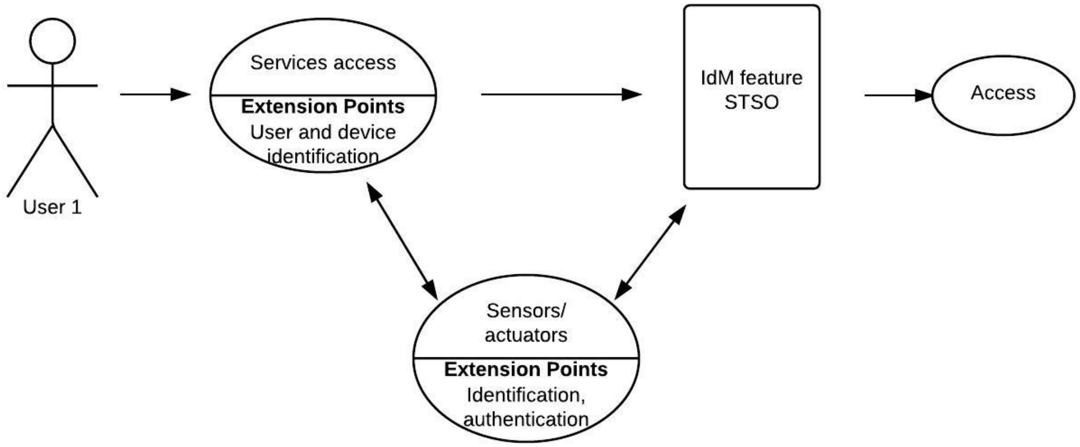


Figure 2.2 Uce-case diagram

In a similar manner, the IdM system might be used when Charlene visits her family's home or when she settles in a hotel for her vacation. In that case the different identities can be used. For example, Charlene would like to access her smart home actuators and activate her air conditioner. In case that she needs to pay for additional services such as massage and tourist excursion, IdM will use her bank account identity.

2.4. Proposed Identification Algorithm based on computing device recognition

A computing Device Recognition (CDR) algorithm for user identification, based on computing device recognition is proposed. It is important to note that the CDR algorithm does not exclude the standard and most typical method for identification - username and password. It can be considered as an additional feature that simplifies the authentication (automatic and less user intervention) but manual authentication can still optionally be used.

The CDR algorithm is presented in Figure 2.3 and discussed below.

The user's types of device identities ($v_n d_m$) are stored in a Smart Sheet (SSh). SSh_x is unique list of devices referring to user *x*. Each device *d* is recorded to the SSh_x list with a reference number within the interval [1-*m*]. For each device in the SSh list, there is a set of different types of identifiers *v,* with a reference number within the interval [1-*n*], which is assigned to the particular device d_m. If a request for identification from one of the listed and registered devices in a certain domain is received, the register automatically starts to search if there are other user devices and how many of them are available in the local domain. The user is able to define the level of security by manipulating the number of the devices needed for a proof of user identity. For example a certain user may create a policy for 3 out of 5 personal devices simultaneous recognition for automatic user identity recognition. The user is a part of the Internet of people whereby he/she plays the role of manager of the rules in the system, regarding his/her preferences and wishes.

The available user's computing devices are counted and written in F'sheet. After that, the algorithm computes the Id index which shows the ratio between the entire devices stored in the SSh and those which are available in the F' sheet at a certain moment. Then, the level of required identification is checked. Here, two scenarios are available - for high and low level of identification depending on the user's or services' rules. If the level is low, the algorithm compares whether Id is bigger or equal to I. In that case, the ratio I is equal to at least half of the declared devices in SSh which must be discovered and recognized.

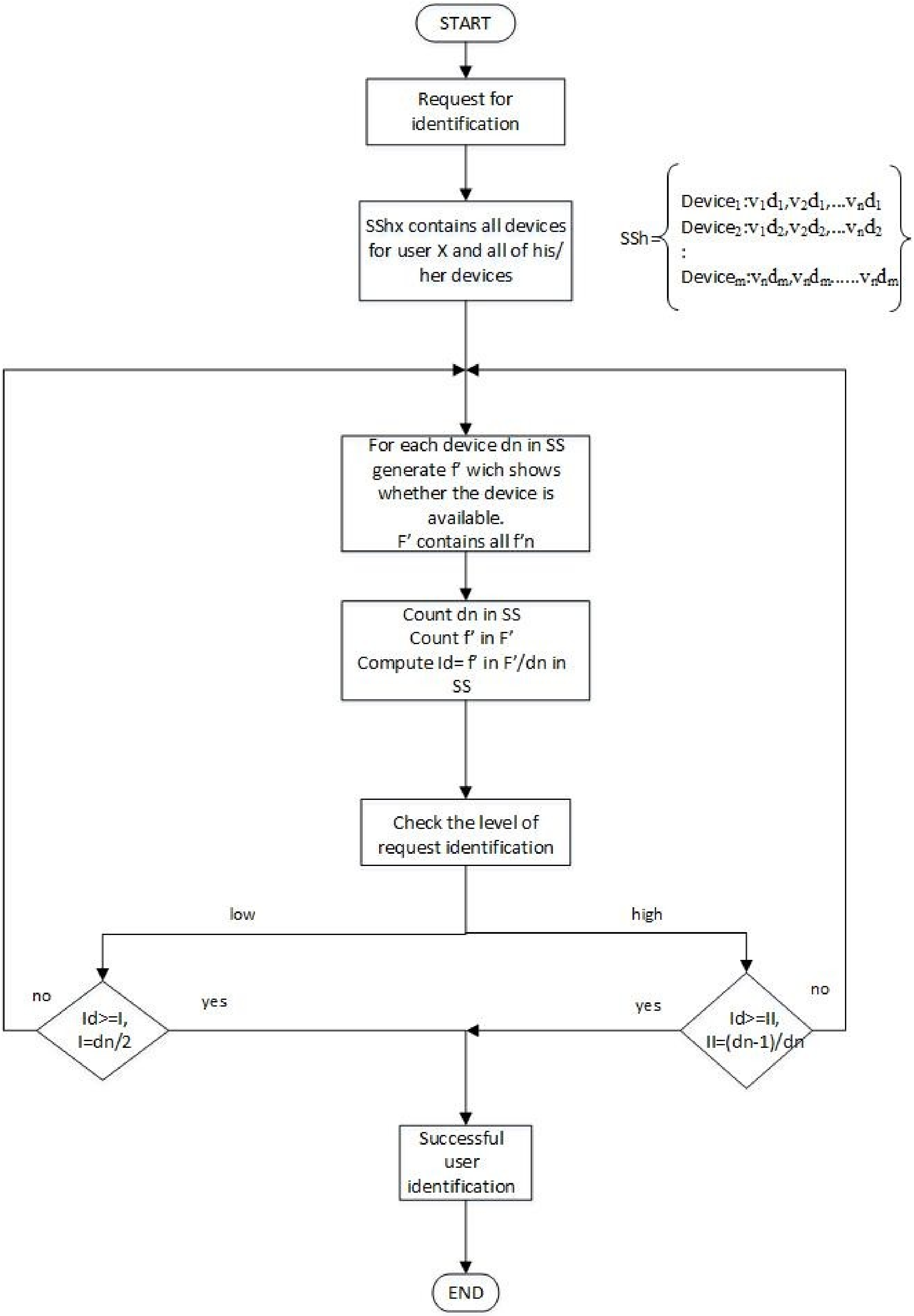

START
Request for identification
SShx contains all devices for user X and all of his/ her devices
SSh= Device$_1$:$v_1d_1,v_2d_1,\ldots v_nd_1$
Device$_2$:$v_1d_2,v_2d_2,\ldots v_nd_2$
:
Device$_m$:$v_nd_m,v_nd_m.\ldots.v_nd_m$
For each device dn in SS generate f' wich shows whether the device is available.
F' contains all f'n
Count dn in SS
Count f' in F'
Compute Id= f' in F'/dn in SS
Check the level of request identification
low
high
no
yes
Id>=I, I=dn/2
yes
no
Id>=II, II=(dn-1)/dn
Successful user identification
END

Figure 2.3 CDR identification algorithm

If that expectation is true, the identification of the user is successful. If not, the process is started again until the timeout for the service expires. If the level is high - that the Id should be compared to II index which allows only 1 of the user computing device to be unavailable. If that expectation is true, the identification of the user is successful. If not, the process is started again until the timeout for the service expires.

Here, a coefficient which defines the identification rate of the computing device is proposed to be used for the assessment of the CDR algorithm.

$$\mathbf{Ircd} = \frac{N_{cd}}{M_{cd}}$$

where **Ircd** is an identification rate coefficient of the computing device

$\mathbf{N_{cd}}$ is a number of identified computing devices *(cd)* related to the particular user

$\mathbf{M_{cd}}$ is a total number of predefined computing devices *(cd)* necessary for the identification

Ircd is equal to the number of identified computing devices related to the particular user over the total required number of predefined computing devices necessary for the identification procedure.

The identification rate of the CDR algorithm depends on the number of correctly identified computer devices, related to a particular user and it must be equal or close to '1' in order to recognize the user itself.

2.5. CDR algorithm analysis

As the CDR-algorithm definition states, it is meaningful that the algorithm does not exclude the standard and well-known methods for login. It is a novel, time and effort-saving automated mechanism for authentication and identification. Furthermore, if one of the user's computing devices is missing (being stolen or lost), the logging feature that is enabled by the algorithm will not be activated and the authentication cannot be performed. Thus, the unauthorized access to the personal user's information or service will be prevented in contrast to password saving on the device.

In case of the user is supposed to possess two or more devices but he/she does not have all of them operational or available at certain moment of requested authentication, the CDR algorithm implies the option for manual password entry, which is predefined by the user. In that terms, the algorithm does not limit or prevent the user' identification at any case.

The proposed coefficient Ircd gives the chance for accessing the algorithm in real situation. Theoretically, the algorithm is promising but because of the lack of implementation, testing and missing information for the value of Ircd, it cannot be concluded that the algorithm works correctly.

2.6. User identification summary

Being connected over the IoT the constantly growing number of communication devices, people and information requires proper identification methods. In this chapter, a brief overview of IoT was described. One of the main processes concerning the identity i.e. identification, authentication and authorization were presented. The significance of the intelligent IdM systems usage was described and a relevant use case scenario was given in order to better understand the identification challenges. As a result, the CDR algorithm for automated and easier process for identification was proposed. For assessment and analysis of the algorithm, a coefficient for identification rate of computing device was proposed.

Chapter 3

Identification schemes in heterogeneous IoT networks

This chapter discusses heterogeneous networks and architectures. The summary of various existing identification schemes and identifier formats have been studied and evaluated, and the research challenges were identified. In the sequel, an identifier format is introduced in this chapter in order to address the objective of manful identity management solution. At the end of this chapter, the evaluation of the proposed identifier format is discussed.

3.1. Heterogeneous IoT networks

IoT consists of uncountable devices, sensors, actuators or simply objects based on the motto “that everything should be connected to the Internet”. IoT enables an ecosystem of smart applications and services, which will be used to improve and simplify the citizens’ live and daily activities by modeling and developing connected systems [6].

IoT and M2M are closely related technologies. IoT can be determined as a basis for providing and supporting connectivity for M2M [28].

3.1.1. ETSI M2M Architecture

The European Telecommunications Standards Institute (ETSI) has developed a M2M communication standards and defined the system’s functional architecture [29].

The M2M high level architecture consists of the following elements: Device, Gateway and Network domain as shown in Figure 3.1. [29].

The Device and Gateway Domain is composed of the following elements:

- M2M Device - it a responsible for running M2M Application(s) using M2M Service Capabilities. By one of the following manners, M2M devices might connect to Network Domain: "Direct Connectivity" connection via the Access network. Example of that kind is device may provide service to other devices which are connected to it and hidden from the Network Domain; or "Gateway as a Network Proxy" connection via an M2M Gateway, which acts as a proxy for the Network Domain towards the M2M Devices that are connected to it. Some of the examples of procedures that are: authentication, authorization, management, and provisioning. M2M Devices may be connected to the Networks Domain via multiple M2M Gateways.
- M2M Area Network: enables M2M Devices and M2M Gateways connectivity. It can include Personal Area Network (PAN) technologies such as Zigbee, Bluetooth®, ISA100.11a, etc. or local network such as PLC, M-BUS, Wireless Meter-Bus (M-Bus) and KNX.

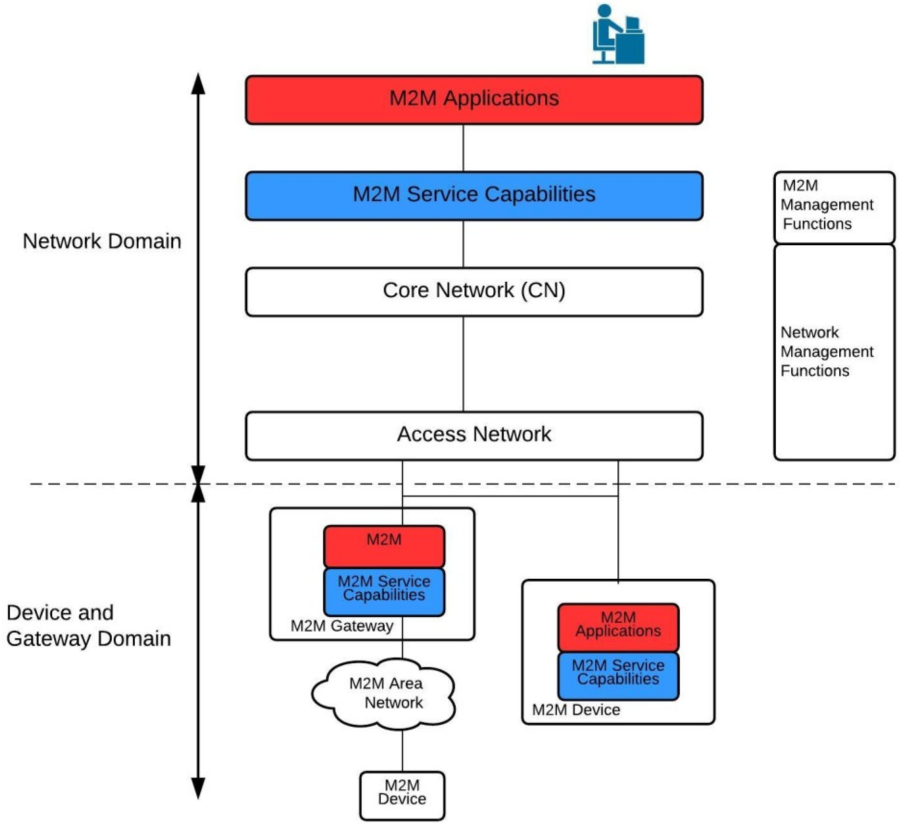


Figure 3.1 ETSI M2M High Level Architecture [29].

- M2M Gateway: responsible for running M2M Application(s) using M2M Service Capabilities. It acts as a proxy between M2M Devices and the Network Domain and it may provide services to other devices (e.g. legacy) connected to it that are hidden from the Network Domain

The Network Domain consists of the following elements:

- Access Network: allows communication between M2M Device and Gateway Domain and Core Network. Access Networks include x Digital Subscriber Line (xDSL), satellite, Universal Terrestrial Radio Access Network (UTRAN), Wireless Local Area Network (W-LAN),Worldwide Interoperability for Microwave Access (WiMAX)
- Core Network (CN): responsible for providing IP connectivity to Internet for M2M devices and Gateways; runs services and network control functions, provides interconnection with other networks and roaming. Different Core Networks such as 3rd

Generation Partnership Project (3GPP) CNs, ETSI Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) CN and 3GPP2 CN offer different features sets

- M2M Service Capabilities: - Provide M2M functions exposed through a set of open interfaces, which can be used and shared different M2M Applications
- M2M applications: run the service logic and use M2M Service Capabilities accessible via an open interface.

As a part of Network Domain are the following two management functions:

- Network Management Functions: these are all required functions to manage Access and Core networks (Provisioning, Supervision, Fault Management, etc.)
- M2M Management Functions: required functions to manage M2M Service Capabilities in the Network Domain. M2M Devices and Gateways management uses a specific M2M Service Capability.

M2M identifiers in ETSI system

In ETSI M2M System a hierarchy of identifiers, keys and sets of procedures are used in order to identify device/gateway node during the establishment of connection between M2M system and node.

The following are part of the model of identifiers [29]:

- Application Identifier (App-ID) - uniquely identifies an M2M Application which is registered at a Service Capabilities Layer. App-ID is used for purpose of interacting with the application. M2M Service Provider is responsible to ensure that App-ID is unique. If more than one instance of the same M2M Application is registered to the same SCL, then App-ID of each instance must be unique.
- Node Identifier (Node-ID) - that is a unique identifier which identifies a node.
- SCL (Service Capabilities Layer) Identifier - (SCL-ID) - identifies SCL uniquely. The M2M System allows SCL-ID and Node-ID to have the same value.
- Service Connection Identifier (CONN-ID) - identifies connection between the M2M Device/Gateway and the NSCL.

- Service Provider Identifier (PROV-ID) - An M2M Service Provider has to be identified uniquely by the M2M Service Provider Identifier. PROV-ID has a static value which is delegated to SP.
- MSBF Identifier (MSBF-ID) - uniquely identifies MSBF. This is a static value assigned by the M2M Service Provider.
- MAS Identifier (MAS-ID) - uniquely identifies M2M Authentication Server (MAS). This is a static value provided by M2M Service Provider.

The identifier format used in the implementation of the system may be determined by the chosen communication technology.

3.1.2. Wireless Sensor Networks

The Wireless Sensor Network is a key technological building block in IoT. Within the context of IoT, the sensor nodes measure data, collect process and exchange information, and perform collaboratively with other sensor nodes and end users, which can be internal or external to the network. WSN architectures converge as a centralized and distributed approach in the IoT application context [18]. In Centralized WSN, the central entity (or a cloud service) has a responsibility of acquiring raw data from the sensors, processing, transforming and/or providing this data in appropriate required format. This kind of WSN does not allow or there is little support of obtaining sensing data directly from the device. In opposite of that, in distributed network, the raw data can be accessed straightaway from the sensors nodes because of processing power and high intelligence level of devices. Dynamic collaboration between end-users and different application platforms is able, no matter that the service provisioning is located at the edge of the network. The using of these two types of WSN in IOT, it is beneficial because the identity and authentication of devices is managed in secure manner. In IoT applications, trusted connection establishment is based on multiple entities (e.g., sensing nodes, service providers, and information processing systems) authentication [30].

3.1.3. Ambient intelligence and assisted living

Ambient intelligence (AmI) is a recent concept being under development in heterogeneous IoT network. AmI is build upon Artificial Intelligence and Intelligent Decision Support Systems (IDSS) where computing devices are used as proactive tools for assisting people with their daily activities. It provides possibilities of acting in unison of wide range interconnected objects, and the process of management and efficient combination of heterogeneous devices and/or things is crucial, thus it is another challenge in the future of computing and communications represented by IoT. AmI is represented by the smart home environment, presence of actual users and their role in controlling and monitoring surrounding devices. In the process of providing services, AmI involves users and their identities [31].

3.2. Identification schemes in IoT

Many different identification schemes in IoT are occurred as a consequence of the ingenuity of humans, committees, and industry. Existing identification schemes in IoT context are presented below in Table 3.1 [32] :

Table 3.1 Identification schemes in IoT [32]

Identification scheme	Advantages	Disadvantaged
RFID Object Identifiers	-An established code structure that can accommodate legacy systems that differ from GS 1 -Has the potential to address any type of application by accepting the domain code structure	-Lack of resolver system to address the different OID structures -No marketing budget for an ISO standard -Centralized in nature
Electronic Product Code (EPC) global	-The potential of the system is based on the GS1 bar code implementation -Possibility of rapid deployment by major retailers -End-to-end code to discovery service system architecture	-Probably restricted to GS 1 domain -At the thing level, limited and uncertain RFID data carrier options -The cost of source marking an entire batch when there are few retailers using the system -Privacy issue could be delay and render post sales IoT features redundant
Short-OID	-Subset of RFID approach that can meet requirements when the entire OID needs it be encoded -Application that needs to encode the OID plus UII	-Lack of resolver system to address that OID structure -Similarity with RFID OID -Lack of domain specific differentiation because the common root may not enable this differentiation

NFC Forum	-Significant infrastructure investment -Potential for ownership by almost everyone	-Air protocol specific -Low data capture integration with other tags -Much similar to 2D bar codes
Handle and OID	-Established system for e-products, but well established within increasing number of domains -Could increase the number of application because of e-product expenditure	-Require additional infrastructure overload for additional application -Isolated from data carriers and it is not suitable for physical objects
Ubiquitous Code	-Well established, particularly in Japan -Resolve process through TRON engine -Potential to operate in parallel with competing systems -TRON engine may be highly useful for other system	-Weak due to reverse logic of the code declaring the data transfer -Not so powerful as EPC global
URL as an identifier	-Established system and supported by choice of browser compared to the other systems -Using alias short form URLs	-Long length and not suitable for data capture -Lack of security
IP address as an identifier	-Enable M2M communication, suitable for long-term monitoring -Applicable for most devices that are part of IoT	-Not suitable to lightweight objects with resource constraints -Scalability problems

The incorporation of such different schemes into an overall structure in IoT is addressed as a one of the big challenges.

3.3. Challenges

Based on the conducted research for currently existing identification schemes, the following challenges concerning the IdM systems for IoT were identified and listed below:

- **User and device identity creation, and management** - the user can have and use different identities in order to access multiple services in IoT. Thus, the IdM should provide identities creation stage for both user and device during the registration phase. Then, it has to be able to introduce them in the authentication phase by accurate selection of identities in fully or semi-automatic way. Therefore, the IdM should manage different identities relationships in order to select the needed identities in a context of accessing service.

- **Authentication of multiple and shared devices** - this challenge is expressed by single user who uses more than one service at a time. The problem could be addressed by SSO in SAML, OAuth etc. The usage of shared devices from different users is another important aspect, and is currently approached by the so called "sand-box" techniques in order achieve differentiation of the users in IdM for eHealth in IoT. Proposed SDSO feature in IdM for M2M is represented by authentication of multiple user's devices where the user can access a particular single service with all of his/her devices after performing initial authentication only on one device. In our case, the user will be able to access multiple services on number of different devices by authenticating himself only to one of those device. The access to connected shared devices will enable gathering contextual metadata and sensors data and will enable user centered responsive services. The enabling IdM feature is introduced by the author as Single Thing Sign On (STSO) and is object of discussion in Chapter IV of the thesis.

- **Heterogeneous network with minimum human interaction** - on a web application level, SSO provides possibility for accessing various services by a singular user sign on process, and as a consequence the user interaction iterations are reduced. The proposed STSO improves user experience within heterogeneous networks by minimizing the number of user's interactions for identification and authentication.

- **Personalized devices** - in order to enable successful communication in the IdM system, the latter should be aware of the devices ownership and in particular, for the user they are linked to.

- **Privacy** - The user's identities are used for accessing one or several services but some of those identities might be used only by a particular service. Thus, IdM should provide mechanism for identity management access depending on the different services which claim to access and use the identity data. Hence, the sharing of user information between different services in the system is not allowed or should follow a certain privacy policy.

3.4. Identifier format proposal

The used identifier in the IdM has to include all related identity information for a certain thing in the system - it means that the identifier has to uniquely define the user, his/her computing devices, domain and non-user interface devices.

The used identifier in the proposed by the author IdM system will be based on the identifier for nomadic thing in IoT by Mahalle [9] presented in the Figure 3.2 Mahalle proposes identifier which assigns ownership to things in IoT. Things in IoT can be represented by people, devices or information, thus it is good to know what the thing is. The things could be distinguished by thing association with unique identifier format and different attributes related to it.[9].

ORI=<OBJECT>,<RESOURCE-1>I<OBJECT TYPE>I<GLOBAL NAMESPACE>I

<LOCAL NAMESPACE> I <UID> I <CID>

Figure 3.2 Identifier format for nomadic things in IoT [9]

Where:

ORI=<OBJECT>,<RESOURCE-1> - Indicates object is Thing or Service

<OBJECT TYPE> - means type of Object (e.g. sensor)

<GLOBAL NAMESPACE> - indicates global ownership/Interface

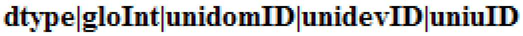
<LOCAL NAMESPACE> - indicates local ownership/Interface

<UID> - means Unique Identification number of device

<CID> - means Context Identity

Mahalle’s format has the following advantages: extended lifetime, scalability and robustness, better performance for end-to-end delay, reduced energy expenditure and improved throughput.

The proposed thing identifier will have the format presented in the Figure 3.3. It is fundamental for the identification in the IdM system. It represented a combination of some partial identifiers.



dtype|gloInt|unidomID|unidevID|uniuID

Figure 3.3 Proposed thing Identifier format

dtype - partial identifier which shows device's type such as sensor, actuator, computing device etc. For human user this option will be 0. This option is required if service needs specific type of measurement (e.g. temperature).

global ownership/interface=gloInt - partial identifier which indicates global ownership or interface and it is required because of the mobility of the devices

local ownership/interface=locInt - partial identifier which indicates local ownership or interface and it is required because of the mobility and location of the devices

unique domain ID=unidomID - partial identifier which defines the area of thing registration. Sometimes, there might be existing domains with the same unidomID register in various IdPs

unique device ID=unidevID - partial identifier which is unique identifier for the device. It can be the device unique number for istance

unique user ID=uniuID - partial identifier which presents uniquely the user coming from a specific domain; the owner of the device

The author aims to improve and simplify the user experience by using the proposed identifier format, serving automatic and easier than ever way of identification and connection to the user. Behind that simple, intuitive solution is hidden complicated integration and realization which are invisible and do not reflect the user experience. User experience might be improved also in a way of using specific additional software components in the process of user profile creation by automatic pre-pending bounding of the uniuID and unidevID related to the current user.

3.5. Discussion

The proposed thing identifier format provides possibilities for global communication over heterogeneous networks in IoT and telecommunication infrastructure by using partial identifier *gloInt*.

In terms of providing device mobility and localization, the identifier contents *locInt* partial identifier.

The partial identifier - *unidomID* represents a unique domain which allows easier way of thing discovery within various different domains. This provides scalability of the system and device mobility over heterogeneous networks.

By using *dtype* as a partial identifier from the proposed identifier format, the utilization of various types of devices will be ensured in the system. Furthermore, the communication in the system will be easier if the user any service requires specific measurement.

unidevID indicates and distinguish each device. That is required in the system in order to be provided and use information to and from the proper device - public or private.

By using uniuID as a part of the identifier, differentiation between users; register in the system will be done. This is required because of the each user personal preferences and the registered to him/her devices and services. This is meaningful for the system in order to provide minimum user interactions possibilities and at the same time exactly what the user wants to access by the particular - device.

The proposed identifier format is not implemented and tested in terms of delay, energy expenditures and improved throughput but it is similar to Mahalle´s identifier format and based on a scientific guess it will perform in the same manner. Theoretically, the identifier is reliable and could be used in IdM system in order to meet the challenges and the requirements.

3.6. Identification schemes in heterogeneous IoT networks summary

IoT enables ecosystem of smart applications and services by providing connectivity of uncountable number of various computing devices, sensors, actuators etc which should be identifiable. In this chapter, a brief description of heterogeneous networks and architectures part of IoT was presented. The existing different identification schemes and identifier formats was discussed, and the research challenges were identified. This chapter introduced an identifier format which could addressed identity management issues. The evaluation in terms of mobility, scalability and thing type of the proposed identifier format is discussed.

Chapter 4

Identity Management Systems

In this chapter, the Identity management system is presented. Furthermore, the different models and currently existing IdM systems are studied and evaluated. The system and user requirements have been defined. In sequel, a concept for the IdM system that addresses identity management of the "thing" is introduced. Furthermore, the main functionalities and actions in the system are described and schematically illustrated by Universal Modeling Language (UML) diagrams. At the end of the chapter, evaluation of the proposed STSO IdM system in terms of comparison to the existing solutions, requirements fulfillment and implementation is discussed. The analysis aims to: find out the strengths of the IdM; identify its weaknesses; analyze fields for further improvements and development of the system from technical and business point of view.

4.1. IdM system overview

Identity Management (IdM) can be explained as a bundle of manual arranged procedures and software components which aims to identify and control computing resources usage, and supports privacy and integrity of data. Different tasks such as certificate generation, role and attribute management, authentication, access control, are involved in IdM. It contains a large number of networking protocols and set of distributed software components. Besides that, the IdM interface to business components, and its management procedure will correspond to law, human resources and business ethics procedures. For design and deployment of successful IdM it is crucial to be taken into consideration the mentioned principles [33].

The ties in the IdM service layer architecture with security and access control need to be interconnected to things. IdM architecture is presented in Figure 4.1 [9].

It shows things as devices with network capabilities ranging from high-end such as mainframes, smart phones to simple devices - sensors. These things may belong to different user spaces and they should be able to collaborate together no matter their heterogeneous. There are different services which need to gather or use information from external or internal sensors in scenarios like private, enterprise and e-Health. Between the things and services layers, in the middle of IdM is middleware layer where the relationships between devices/things, and services are securely managed [9].

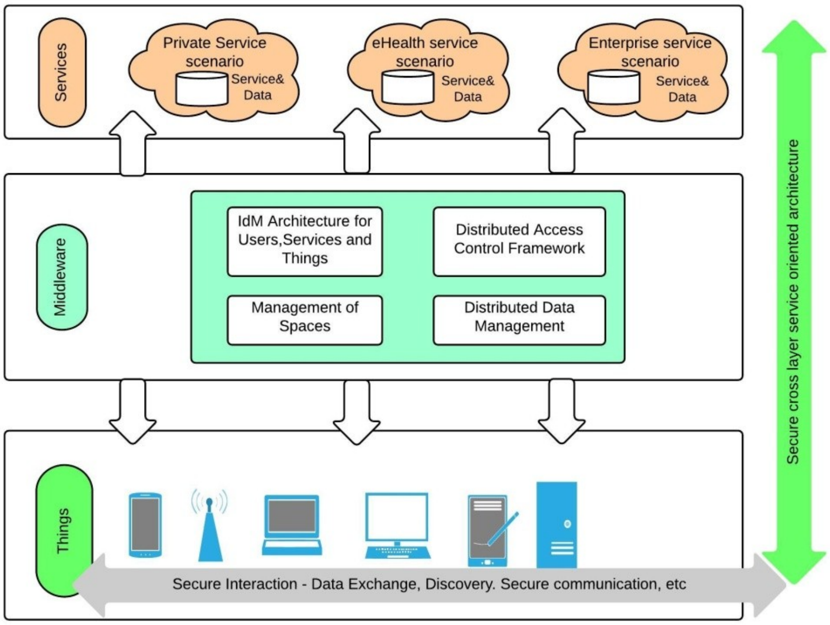

Services
Private Service scenario
Service& Data
eHealth service scenario
Service& Data
Enterprise service scenario
Service& Data
Middleware
IdM Architecture for Users,Services and Things
Distributed Access Control Framework
Management of Spaces
Distributed Data Management
Things
Secure Interaction - Data Exchange, Discovery. Secure communication, etc
Secure cross layer service oriented architecture

Figure 4.1 IdM Architecture [9]

The design of IdM must aim to balance between protocol overhead, software characteristics and security in order to operate successfully in mobile and wireless systems, thus to reduce overhead benefits for all business application processing [33].

4.2. IDM system models

4.2.1.1. A centralized IdM system model

One type of IdM system is a centralized IdM, where the roles and relationships are strictly defined. In that kind of system, one Identity Provider (IdP) manages the authentication of the user, and the identity information is used by one or more than one Service Providers (SP). A centralized IdM system has to be trusted by both - its users and SPs. SSO feature can be enable and respectively the user's efforts will be reduce when he/she wants to use new services in the same domain as the services which they are already used. The creation of one or more virtual identities is allowed for the user. IdP creates also virtual identities which are not linked to each other [34].

4.2.1.2. Isolated IdM system model

One IdM system is isolated if it requires to the services to contain their own IdM. To utilize such a system, a user creates a *virtual identity*, representing only a subset of the entire user's identity (all the data known about the user) necessary for a user's actions in a particular domain of a service [34].

4.2.1.3. A federated IdM system model

The concept of federated IdM system is to conduct the identification of the user on the whole web level, and the user is able to distribute his/her digital identity across multiple domains. That is more known as SSO, reduces the effort, enables access to multiple web services based on single once sign in of the user. The cost of the development is reduced because of the authentication is performed by IdP [35].

4.3. Heterogeneous IdM systems

The Section 4.3 presents the different IdM systems bundled in two categories device- and user-oriented.

4.3.1. Device-oriented systems

In this section, different IdM systems bundled in two categories device- and user-oriented are presented according to their main focus on the end-user - human or another device.

4.3.1.1. DNS and ONS

The Domain Name System (DNS) is a device-related, hierarchical naming system. It is built on a distributed database for any resources connected to the Internet or a private network. DNS is liable to spoofing and authentication problems and it is not suited for critical infrastructure [36].

Based on DNS functionality, Object Name System (ONS) stores Name Authority Pointer records containing location of objects' meta-data information refer to by identifiers. Obtaining of device meta-data might be done by sending regular DNS queries because of relation to DNS. Combination of operations of ONS and additional protocols is must in order to be found and obtained meta-data location storage.

The way of object identifiers' obtaining is not specified in ONS. Since the use of Electronic Product Code (EPC) to identify products, it potentially identifies the objects by using RFID tags and bar-codes. According [37] EPC Discovery Service has replaced ONS because the latter is unsecured and deprecated [37].

4.3.1.2. Cooltown

Another device-related system is Cooltown, which is RFID-based and uses Infra-Red (IR) and RFID to transfer thing's identifiers, i.e. links to web-pages representing them, enabling so-called *web-presence.* The web-pages are either hosted in the items themselves, e.g. in connected devices, or external web- servers. These web-pages provide information and services related to the represented entities. Furthermore, since entities are web-present, the approach actually treats entity meta-data as identities. In the broad sense, the system provides an AmI functionality, where a user may interact with locally available services presented by other entities in the environment using his/her device, e.g. a mobile phone. Similarly to OID-based approach, Cooltown is based on DNS services, thus creation of new identifiers is rather restricted.

4.3.2. User-oriented systems

In this section, the information regarding systems mainly oriented and focused to the end-human user are presented. They aim to offers easier and newly ways of user identification.

4.3.2.1. Open ID, SSO and Security Assertion Markup Language (SAML)

Open ID (newest version 2) is a decentralized IdM system designed to enable and provide a user with SSO feature for access to websites and applications, and providing the user with it. Three parties are being involved: (1) a User Agent (UA), controlled by a human user; (2) a Relying Party (RelP), which provides the service; (3) an OpenID Identity Provider (OIdP), which authenticates the user and delivers his/her personal information to RelP [11]. OIdP is identified by a URI. The user of OpenID technology should select and register in a OldP and obtain an Identifier called User-Provided Identifier (UPID), needed for later authentications.

An OpenID identifier is usually in the form of a URL. The connection between the digital and physical identities is logical, which will mean that a physical object can have more than one digital identity. In addition to URLs, OpenID identifiers can be represented by i-names, which are a form of the XRI standard [35] .

A user may create and manage several identity profiles at the same OldP and keep control of his/her private date by selecting which specific identity to provide to the RelP. The trust mechanisms for relationship management between ReIP and OIdPs are not ensured by OpenID [11].

The authentication process in an OpenID login supported websites, for example, is initiated by a user and the RelP discovers the OldP based on a given identifier to find the endpoint URL for OIdP. The RelP validates and analyses the response and either denies or grants access to the service.

The Security Assertion Markup Language (SAML) is an Organization for the Advancement of Structured Information Standards (OASIS) open standard for representing and exchanging user identity, authentication, and attribute information [38]. A SAML assertion provides vendor-neutral terms of information transfer between federation business partners. And thus to enables enterprise authentication. The assertion involves three parties Figure 4.2: (1) SP, that provides a service valuable to the user; (2)UA, used by a human user to obtain access to a service provided by a SP and (3)IdP, that provides SP with identity information related to the subject.

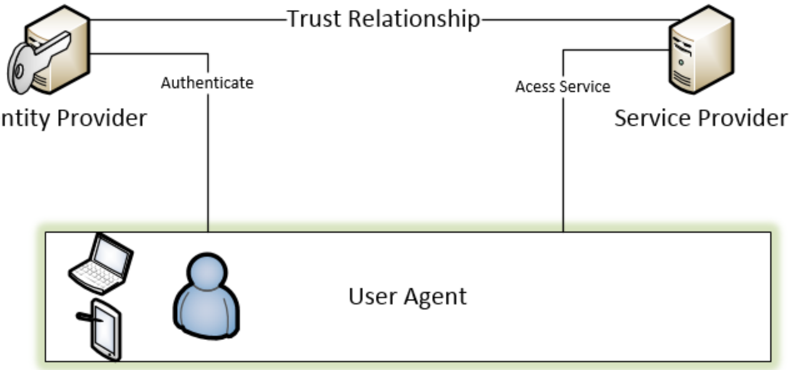


Figure 4.2 SAML [38]

The earlier SAML versions 1.0 and 1.1 are now outdated, thus further discussion addresses SAML version 2.0, comprised of the three following components (Figure 4.3) [39]: (1) Protocol messages that encapsulate data, e.g. security assertions; (2) Name specification bindings, for transporting SAML messages; and (3) A specified complete profiles, combining bindings that can be used to perform authentication and authorization.

SAML assertion specifies message formats, bindings and profiles. Bindings [39] define the procedures of message sending, and profiles [39] describe a combination of bindings applied for communication between specific parties.

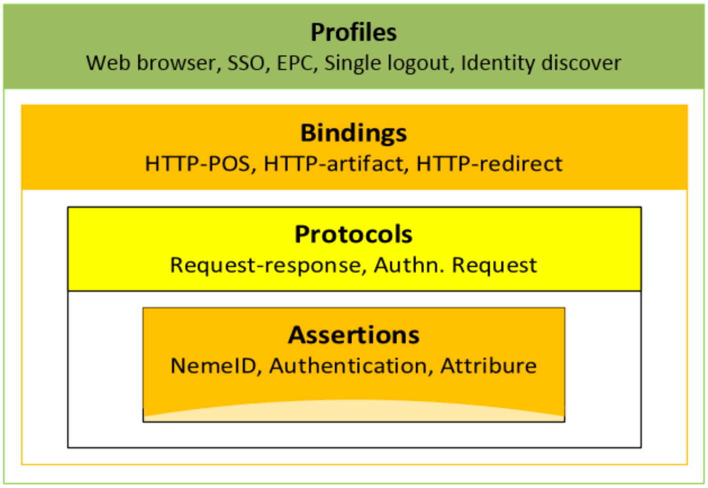

Profiles
Web browser, SSO, EPC, Single logout, Identity discover
Bindings
HTTP-POS, HTTP-artifact, HTTP-redirect
Protocols
Request-response, Authn. Request
Assertions
NemeID, Authentication, Attribure

Figure 4.3 SAML components [39]

Messaging in SAML is based on Extensible Markup Language (XML) format. The generic message type in SAML is security assertions, which contain statements about a subject's attributes and rights. A single assertion message contains one or more statements of the following types: (1) Authentication Statement - providing information about the authentication process (for example, time , method and result of subject authentication); (2) Authorization Decision Statement - to indicate whether access to the requested resource has been granted; (3)Attribute Statement - to provide more detailed information about the authenticated subject.

4.3.2.2. OAuth 2.0

OAuth 2.0 addresses currently web-based needs and defines a protocol for third party service authorization, i.e. Client, to act on a resource owner's behalf when performing certain actions on a resource stored in a Resource Server. In OAuth2, security is provided by Hypertext Transfer Protocol Secure (HTTPS) protocol, depending on Transport Layer Security (TLS) [40].

OAuth2 does not use HTTP POST messages. It uses only HTTP redirects in UA for message forwarding among parties and in that way it supports mobile clients (applications) which do not have access to POST messages. This is an advantage in comparison to OpenID and SAML 2.0 [40].

OAuth2.0-based authorization process involves the following parties [41] :

- Resource Owner (RO): an entity possessing certain resources and willing third party Client to access them/resources
- Resource Server (RS): a server where the resources are contained.
- Client: a third-party application needs to execute action on a resource in RS
- Authorization Server (AS): a server which is responsible for the RO authentication and issuing authorization tokens to Client allowing operation on a resource.

Single entity can execute the roles of RS and AS, and their relationship and interaction is beyond the scope of SAML.

4.3.2.3. OpenID Connect

OpenID Connect addresses many of the same issues as OpenID 2.0 but in a way that is application programming interface (API) - friendly, and supports native and mobile applications.

OpenID Connect proposes a definition of access to user's identity information which is not issued in OAuth2 [42].

OpenID Connect is "a simple identity layer on top of the OAuth 2.0 protocol. It allows clients to verify the identity of the end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user in an interoperable and REST-like manner" [42].

OpenID Connect provides authentication functionality and is an extension of OAuth2. Based on OAuth2 definition, the roles in OpenID Connect are defined and specified tree message flows: the Authorization Code Flow, the Implicit Flow, or the Hybrid Flow involving different endpoints for issued tokens. Figure 6 gives an abstract overview of the OpenID Connect protocol flows [42].

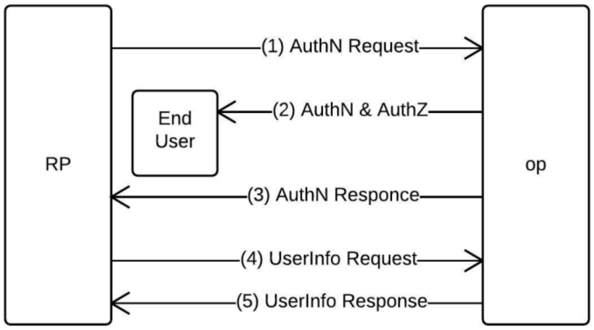


Figure 4.4 OpenID Connect communication flows [42]

1. The RP (Client) sends a request to the OpenID Provider (OP).
2. The OP authenticates the End-User and obtains authorization.
3. The OP responds with an ID Token and usually an Access Token.
4. The RP can send a request with the Access Token to the UserInfo Endpoint.
5. The UserInfo Endpoint returns Claims about the End-User.

Identity information access is managed by the UserInfo End point which provides the user identity-related information upon request from RelP possessing access token. The returned identity information depends on the access token and the acquisition setup [42].

4.3.2.4. oneM2M - Standards for M2M and IoT

The wide range of capabilities of M2M communications have triggered a number of standardization processes involving a some of the main standardization bodies like ETSI and 3GPP, which has led to incompatibilities and isolated structural solutions. For addressing the problem of ETSI alongside with together organizations founded the global M2M organization, oneM2M, aiming to establish a common global M2M communication service layer [43]. In addition the coordination of development processes associated with the current M2M service layer standards and common features has been addressed. With a standardized service layer, oneM2M aims to define methods for various functions, M2M protocols, APIs, reachability, discovery and management, security and privacy. oneM2M expects to contribute for minimizing the deployment expenses, simplify the process of application development, reduce the time-to-market phase and prevent overlaps of existing or developing standards [43].

4.3.2.5. My personal adaptive global network (MAGNET)

"My personal Adaptive Global NET" is a project based on a user-centered approach aiming to improve the quality of life and emphasis on user-centricity, personalization and personal networking. MAGNET envisioned that the users will be supported by a personal network (PN) connected devices which can be private, shared, or public and adaptable to the quality of the accessed network. In this context the users are enabled to project their actions regardless of location through remote personal devices [15].

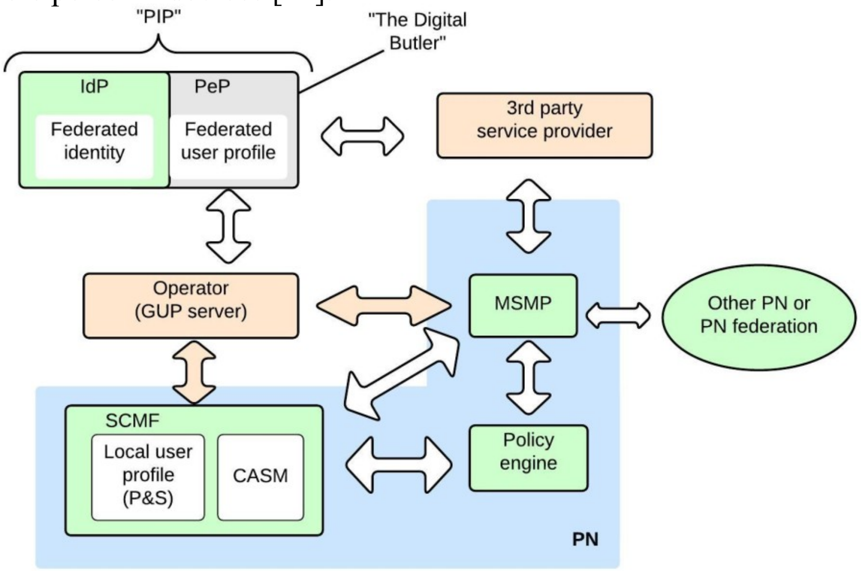


Figure 4.5 MAGNET overview [15]

MAGNET adopts the SSO and federal identities and further combines that with Me “Digital Butler” idea leading to the concept of Personal Identity Provider (PIP) that manages the user profile. A specific set of user profile information almost autonomously makes a complete selection of services, application and devices for each network, access and context situations. The management and storage of user profiles’ information is communicated through the MAGNET Service Management Platform (MSMP) [15].

Me opportunity to access relevant information from a single point of entry with a single sign-on function is addressed in MAGNET Beyond, and a key issue is a provisioning of service.

A user logs on to authenticate himself to an identity provider. A user can hold credentials from multiple IdPs and a "Federation" of IdPs is also possible. The different service providers, however, are not allowed to communicate any information about the user between each other. They can exchange information relating to this user only with the IdP that can access the MUP for relevant data, if it is available. LA can grant access for a service provider to offer services to MI identified user or a representative of the user - say a sort of Digital Butler" if a certain service provider is accepted by either the IR or the user. The concept of personalizing services making them value-added is not new but it is important [15].

4.3.2.6. Identity Management Framework towards IoT

P. Mahalle proposed one layer IdM system with set of processes for IoT presented in Figure 8 in his dissertation [9]. IdM is defined as a management of identity followed by identity authentication and attribute authentication. The author introduces a separate context identity (CID) depending on the context and supporting context awareness and applying namespace dependent identifier to ting. The key milestones in the proposed framework are Context management, identity binding, identity mapping and lifecycle management which uses credentials and identities as an input [9].

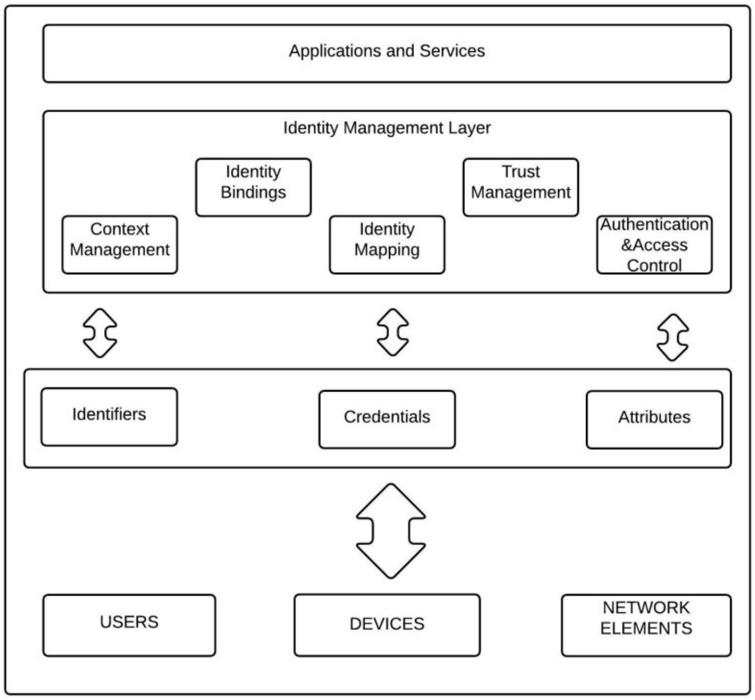


Figure 4.6 Framework for IdM in the IoT [9]

As a conclusion, the author claims that the proposed IdM is effective in IoT. The user relationship in that IdM is omitted and addressed as a future work.

4.3.2.7. Identity Management in the Internet of Things: the Role of MANETs for Healthcare Applications

Caroline Chibelushi [44] proposed user-centered and modular IdM framework for healthcare in IoT which is presented in Figure 9 Each module in the proposed IdM is designed to work on its own or in conjunction with others.

The proposed IdM system claims to be suitable, and provides possibility of sharing devices and seamless interaction in IoT domain. The Identity module involves the following parties: Device ID, IP, and Use ID, where User ID consists Device ID and user type. The Sandbox module is used in order to separate the individual data within the shared device, because that is important and sensitive, especially in e-Health context. In addition, the used sandboxing technique offers a possibility for adding data security for things by isolating individual personal content. The Context module helps to be provided personalized service to things by tracking the identity of Things and users in dynamic way [44].

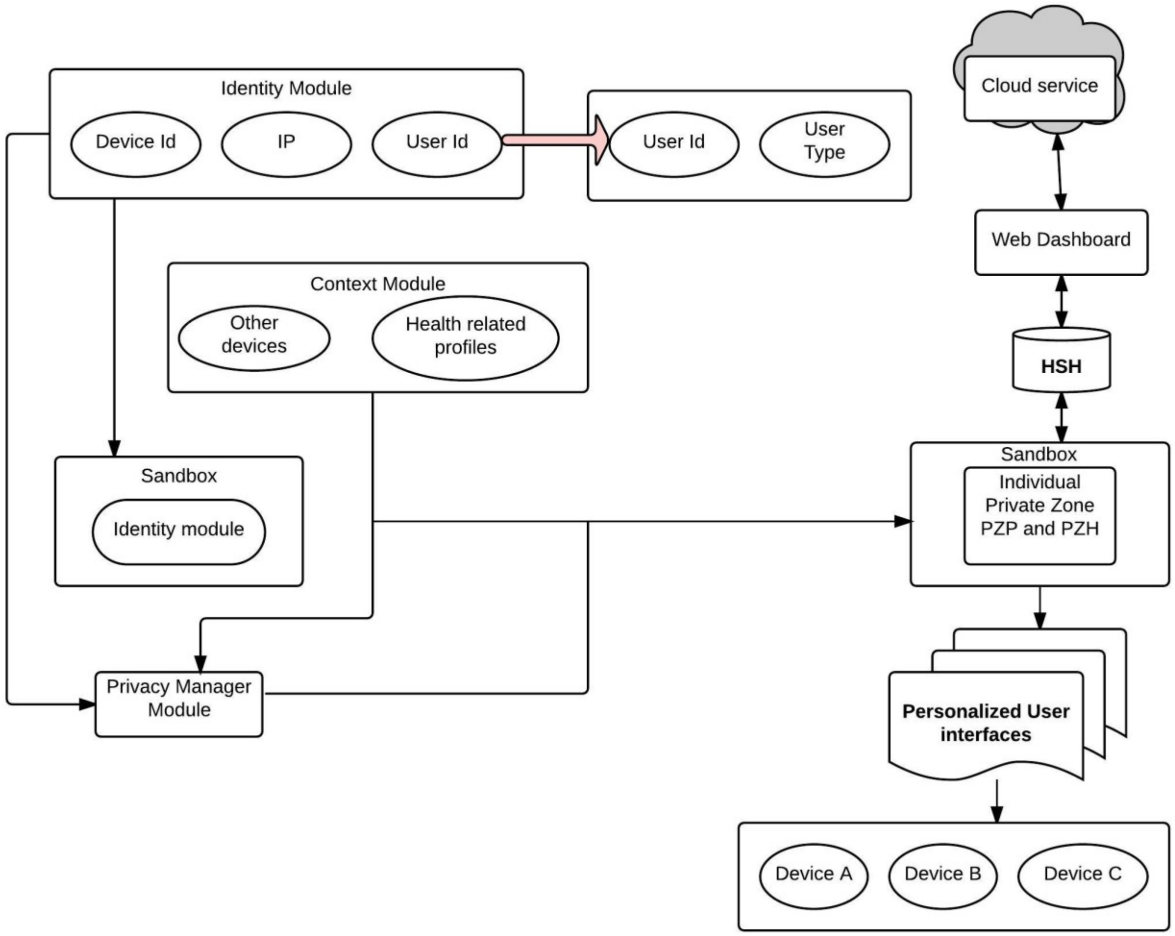


Figure 4.7 IdM-MANET framework [44]

The *privacy management module* creates dynamic privacy policy in IdM and provides personalized user interfaces and access rights information for identified users within the framework. Information is released based on required functionality and only when that is needed by proposed algorithm which is not further investigated in the thesis. User interface is personalized where the user can take a decision about reducing or not information, and shows information available to other nodes. Each identity can be mapped to more than one profile. The proposed IDM framework in e-health context accepts the assumption for wirelessly connected healthcare devices. Different users' identities are separated in a clear way when the share device is used. The proposed IdM system does not address device to device communication issue.

4.3.2.8. Identity Management in M2M networks

A user centric IdM for IoT whereby the identity is based on a Single-Device-Sign-On is proposed by Do Van Thuan [45]. A distributed and federated IdM model incorporates the following: users, devices, Service Providers (SP) and Identity providers (IdP) [46].

The IdM consists the three main components [45]:

- Device Subsystem (DS) - installed in a user's devices, providing authentication functions and access services based on certain user identification.
- Identity Provider Subsystem (IdPS) - stores identity data and authenticates user, device and services also. It is located on server of Identity Provider's server and can be private or public.
- Service Subsystem (SS) - located on Service Provider's server, responsible to enforce the control of service access and to authorize authentication to IdP

The device will present identifier which is user dependent to the Service Provider in order to be authenticated and access the service [45].

The IdM addresses the interaction and collaboration between people and devices, based on users' identities and "relationships between users" [45]. The author does not describe the process of communication between the computing devices how they can be connected to sensors networks.

4.4. IdM system requirements

Alongside with the challenges that the IdM faces, there are many user requirements which the IdM system has to address. Talking about the user we refer to a human user who is using proposed STSO feature for identification. Based on the conducted literature research [6] [8] [14][17][19] and analysis the main requirements influencing the STSO integration in IdM systems are summarized into two main groups as: (1) Generic system requirements and (2) Generic user requirements.

4.4.1. Generic system requirements

The following requirements should be addressed from the proposed STSO integrated IdM system point of view:

- **Flexibility** – to enable support of various network devices.
- **Scalability** – to scale easily to envisioned use-cases and provides global communication through discoverable identifiers which are unique within various domains.
- **Extensibility** – to provide integrity and proper APIs for integration of novel for the system devices.
- **Reliability** – to provide reliable communication on-time reaction, thus IdM should be familiar with the correlation relationships.
- **Privacy** – to keep and protect the personal user information from unauthorized access.

4.4.2. Generic user requirements

Taking into consideration the end-users expectations and needs both from technological and personas perspective the main user requirements that influence the STSO integrated IdM system are:

- **End - user as an owner of the rules operating smart things -** As a part of the IoT ecosystem, the end-user takes an active role by informing about his/her needs, providing feedback and rules the actuators individually [8]. The STSO integrated IdM system will provide features for profile personalization and based on that will run selected to the user services.
- **New responsive services at any time (always)** - the offered services shall answer and support the end-user needs no matter time and place. By specific mechanisms for communication between all of the things in IoT, the proposed IdM intends to serve always responsive services, composed as a running-time and specific user' context running services [8].

4.5. IdM vision

Based on the IoT mission for connection of each thing and in order to meet the user expectation, the proposed IdM is user-centered. The vision of the system is *to provide an fully functional human-user oriented STSO and IdM system for IoT.*

The IdM should be able to recognize the unique device identifiers and through STSO to automate exchange of the ownership information, features and capabilities between devices. STSO should allow interoperability of devices within heterogeneous networks and provide the necessary authentication and communication mechanisms for minimized user iterations.

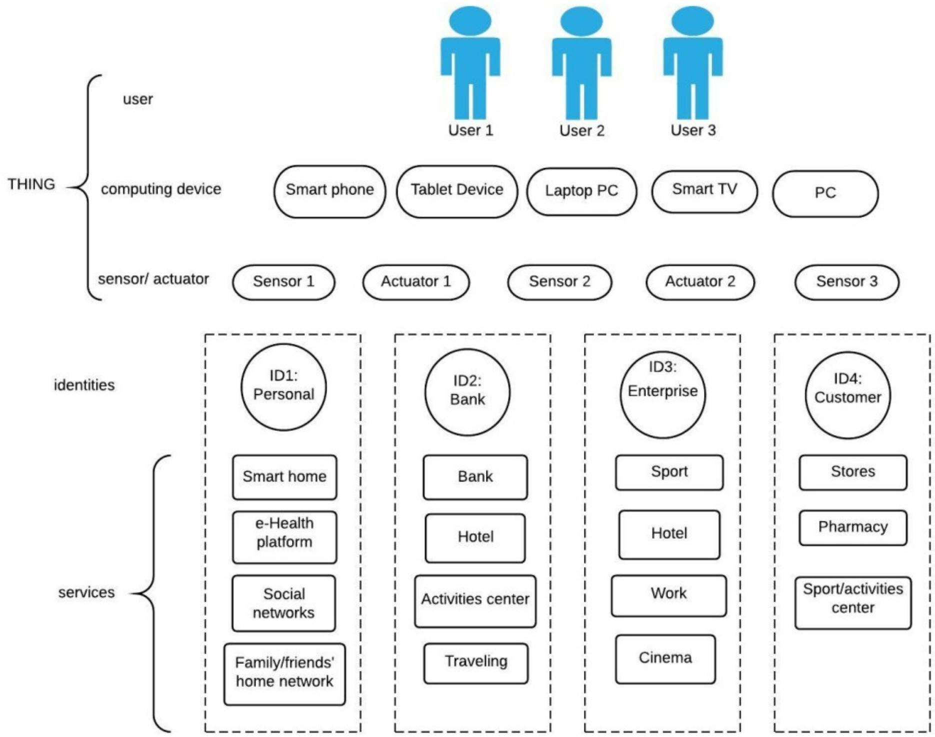


Figure 4.8 Services access by multiple identities

The vision of system configuration is shown in Figure 4.8. It involves the different user's computing devices (smart phone, laptop PC, tablet) which are uses to access multiple services by providing his/her personal identities to device(s). That is required because the user should be recognized by the service and allow multiple services authentication. The identities and services association are represented by the rectangles in the given Figure 4.8.

4.6. IdM system proposal

The proposed identification algorithm in Chapter 2 and identifier format in Chapter 3 will be used in the proposed IdM system in order to meet the requirements and the desired vision.

4.6.1. Entities of IdM system

This section presents entities further described with identities which participate directly or indirectly in the communication. The physical infrastructure of the system together with the physical entities is presented in 4.6.1.1. In section 4.6.1.2., the logical entities are explained further in more details.

4.6.1.1. Physical structure and entities

According to our vision of IdM for identification of the user and distributed his/her digital identity across multiple domains for providing always response services, the proposed STSO IdM will follow federated IdM system model. The high-level system architecture is represented in Figure 4.9., given below:

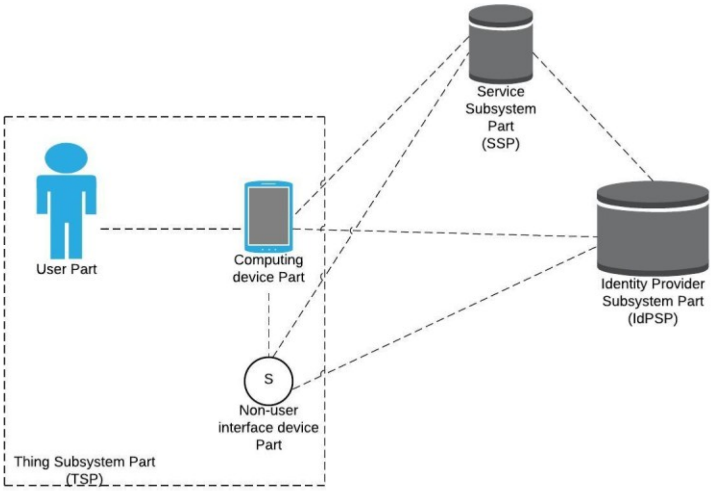

Service Subsystem Part (SSP)
User Part
Computing device Part
S
Non-user interface device Part
Thing Subsystem Part (TSP)
Identity Provider Subsystem Part (IdPSP)

Figure 4.9 High - level IdM system structure

The proposed IdM system architecture involves the following physical entities of the system:

- **Thing Subsystem Part (TSP)** - it represents the “things” in IoT such as users, smart computing devices, sensors and actuators. All of them take an important role in user identity process by providing identities to Identity Provider Subsystem Part (IdPSP). TSP is divided into three separate subsystems: (1) User as a Part, (2) Computing device and (3) Non-user interface device (sensors/networks) further explain below:

1). ***User as a Part (UP)*** - in the proposed IdM system, the user is an actor, being a part of the system, who access multiple services by using his/her device(s). User identity data is obtained and provided by IdPSP.

2). ***Computing Device Part (CDP)*** - it is a functional layer residing in a user device and serve for providing middleware functionalities for the system. From security point of view, this part is needed to prevent unauthorized data modification and corruption.

3). ***Non-user interface Device Part (Non-userIntDP)*** - this part is responsible for collecting accurate information from personal and/or shared non-user interface devices regarding users' needs. In that way, it supports SSP to provide always on time responsive services to the users.

- **Identity Provider Subsystem Part (IdPSP)** - the responsibility of the IdPSP is to storage all the identity data. In addition, it is also responsible for the user, device and service authentication. Also, access to the non-user interface devices is managed by IdPSP. It can be remotely or locally located and one of the main benefits is that the IdPSP can provide communication and different functionalities automatically.

- **Service Subsystem Part (SSP)** - is a part of the proposed IdM service layer that enables authentication of a user or "things" both for local or remote services.

The design of the proposed IdM system allows multiple IdPSs management by multiple IdPs. IdPSPs provides identity storage information, features for searching and discovering from a device perspective in an easier way and thus the latter is able to establish dynamic connections.

The regular user can create a private subsystem of identifiers for his devices and established identities, which can be further provided to an IdPSP to manage them.

Referring to the remote storage of data and IdP designed as a cloud service, it gives the option for IdM to enable mobility of the devices between different locations (e.g. from home to the office, between two homes, etc.), global public access, system scalability, etc. From a privacy perspective, it could be assumed that the privacy is improved as a function of the overall cloud trust model. In the proposed IdM scheme, authentication is required for both the user and the service.

4.6.1.2. Logical entities

Obtaining of related data information is crucial for establishing communication between multiple shared devices. Thus, logical entities management mechanism is used.

1. Things are divided into 3 groups represented respectively by: a human user, computing devices and non-user interface devices.

- User - an actor, being a part of the system, who utilizes multiple devices in order to access one or multiple services such as social websites, smart home, e-health portals etc.

- Computing device - it represents the hardware part for communication with other hardware parts through a given channel for data exchange. Those devices are typically managed by human users and that is relevant for our IdM system. Computing devices can be private or shared whereby one device is used by different users in different periods of time. The final decision for the executed and operating services/resources through certain device is driven by the user.

- Non-user interface device - are electronic devices (in most cases sensors or actuators) which have basic data processing hardware, gather information or operate and communicate also through certain communication channel (Wi-Fi, Bluetooth, ZigBee, etc). Those devices usually are not directly manipulated by human users. In our IdM system, non-user interface devices are managed by IdPSP. Those devices can be also private or shared such as computing devices.

2. Domain - In context of IoT, the domain is the area where the things (devices or users) operate. It can be a specific environment or service which provides identity or defines utilization scope. The domain spaces provide access related decisions based on the information about the "thing" and in addition they can define specific SP for user or device authorization checks in IdP and afterword to forward the authorization to the service itself. This defines two step processes for authentication: first for a Domain and second for the SP.

3. Service Provider - that part provides required services to the users.

The relation between the entities in the system can be easily observed- a certain user can operate with a given computing device, and use specific non-user interface device information. All of those devices can represent a certain domain/user. That information is required to be taken into consideration in the access decision-making process. Based on that, in the proposed IdM system we use identifier which represents a specific user who utilizes certain things from a given domain. That identifier is combination of a single user-thing-domain

4.6.2. IdM system features

The system architecture diagram given on Fig 4.10 incorporates a number of the proposed IdM system components and at the same time leaves open features for future implementation of new cases (that are not and object of discussion within the thesis). The detailed process for the software artefacts development and implementation goes beyond the scope of this document and need further definition and clarification.

The IdM is envisioned to be designed and deployed as cloud operating public service. The "thing" identity in IdM component is managed and performed by Identity Manager and it involves IdPSP, data processing and non-user interface devices actions. The mentioned Identity Manager administrates and manages relations to a given domain and it differs from Identity Provider which provides identity management infrastructure. Identity is created by and in the "things". User as a thing and actor in IoT creates his identity which is stored in IdPSP by using personal or shared devices.

Registration phase: Before utilizing the IdM functionalities, the things' identity has to be stored in IdPSP by creating Smart Sheet (SS). The data flow procedures for the identification at the local IdPSP are not investigated and clarified in the thesis. The system should communicate by reachable IP address, respectively in the proposed identifier format that is *gloInt*.

Domain creation phase and obtaining a *unidomID*, when the user or an organization would like to register for utilizing IdM.

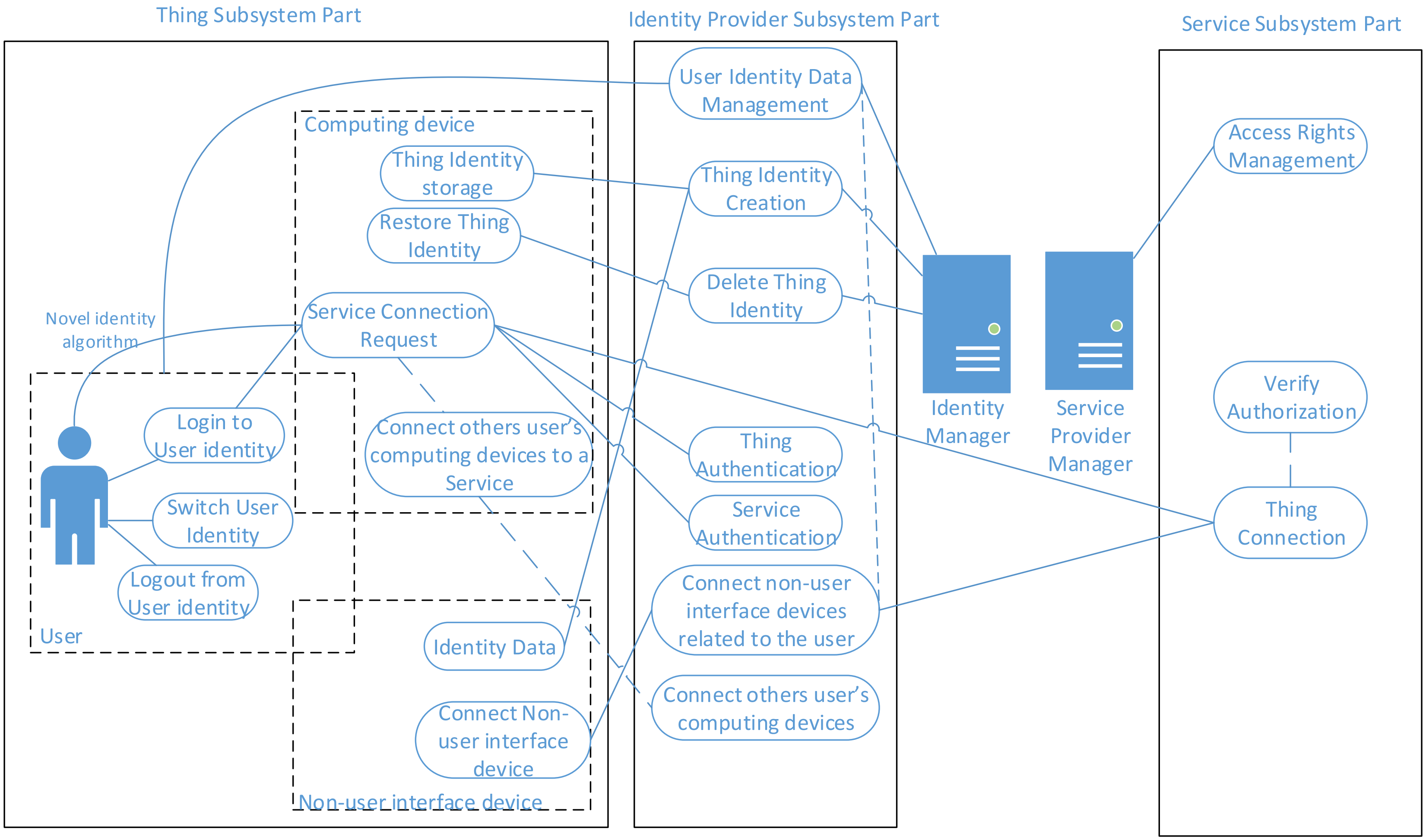


Figure 4.10 Architecture components and functions diagram of the system

After the domain creation, the thing identities creation takes place and involves user identity creation performed by *Identity Manager* and devices identity creation performed by IdPSP.

- The user is identified by *uniuID*. The user creates rules for his identity management procedures by using his credentials. The credentials are bounded to the user identity as a part of the profile creation process and are used for authorized personal data and settings management. The most widely used type of user credentials is the username and password combination, biometric identification data. The author introduces a novel mechanism for user identification based on user devices identification (see Chapter 1, Section 2.4.).

- In the process of computing and non-user interface devices identity is created in IdPSP component and it is similar to the user identity creation stage. The mentioned devices are identified by device type information *dtype* , *unidevID*, and *unidomID* information. As an object can be considered anything or services which determine non-user devices related to a certain user regarding his/her preferences or service subscriptions.

Detailed explanation of each of the components involved in Architecture diagram of the system follows in the current section.

Thing Subsystem Part components:

The TSP is deployed within the locally operating devices and provides functionalities similar to a gateway but with more dedicated for identity and services access management functions. The most viable for the proposed by the IdM system are selected and discussed by the author. The component is open and scalable for future definition and implementation of functionalities related for IoT identification in different context or use case scenarios. The key TSP functionalities and their correlation model for enabling the proposed IdM system are described as follows:

LogIn to User Identity: *User* enables his identities *uniuID* to the computing device which sets user identity by *unidevID*. Afterwards, the computing device will provide those identities in the process of authentication in order to access the requested service(s). The process of providing the users' credentials to the device is out of the scope of this thesis.

The author proposes a novel algorithm for automatic user identification based on a method for user computing devices recognition. By using the proposed user identification algorithm based on availability and recognition of computing device identification, STSO feature is activated automatically and all of the other things are connected in an automated manner without any need of providing separate user credentials. Detailed explanation of the algorithm is presented in Section 4.3.1

Logout from User Identity: The action of "identity logout" is performed when the user wants to disconnect his currently active devices or applications from the operating services under the confirmed identity. The logged out user will be requested to perform the login procedure for authentication of his devices in order to renew access to the available infrastructure or services.

Switch User Identity: The need of user identity change is executed by ***Switch User Identity*** function whereby the user may be required to provide specific set of identity to a given service or another user who utilizes the shared devices. If that component is activated, the user has to perform full login to User Identity procedure mentioned above.

***Thing Identity Storage*:** it stores the same information in the computing device as in Thing Identity creation use case related to the user's devices (*dtype*, *unidomID, unidevID, uniuID*).

Restore Thing Identity*:** the action is performed when the user does not consider a certain device suitable for using it in the ***Login to User Identity use case. Respectively, the information related to the given device is deleted in the IdPSP register.

Service Connection Request* :** This use case procedure enables manual or automatic request for service connection through user's computing device. This component is the main consumer of the STSO functionality and it enables multiple services and devices to be accessed upon request without need of manual typing of user credentials to all of the consumer devices and applications. The ***Service Connection Request component handle the services access provisioning based on the user identification and enables the identified devices to access both remote and local services.

Connect others user´s computing devices: after thing authentication, the rest of the written in the SSh (Smart Sheet) computing devices are connected manually or automatically regarding the user's preferences.

Identity data in Non-user interface device: obtain and provide data to the IdM in order to claim which non-user interface devices are related to the particular human user. In that case, the object and object type information is collected.

Connect Non-user interface devices: after authentication of the user and his computing device, the related non-user interface devices (part of SS for the certain user) are automatically connected based on STSO feature in order to responsive services.

Identity Provider Subsystem Part components:

Identity Manager: The component creates, manages and deletes thing identities within the IdM system.

Thing Identity Data Management**:** this use case enables management and administration of things (user, computing and non-user interface devices) related data information and/or domain entities. It can be performed either from a user as a owner of the rules or by ***Identity Manager*** as a core authorized management component. User full-provisioning identification and verification process, needed to activate this action are out of the scope of the thesis. That has to be an object of further discussion and clarification in the process of implementation.

Thing Identity Creation: It is an use case procedure for storage identity information of thing (*dtype*, *unidomID, unidevID, uniuID*) in IdPSP. That information includes security data and is used in the process of communication between device and IdPSP.

Delete Thing Identity*:* this use case performs the action of deleting the thing's identity information in IdPSP if the user does not consider a particular device suitable for using it in the ***Login to user identity*** use case and executes the use case ***Restore Thing Identity***.

Thing Authentication**:** the action performed authentication of the device of the user and check if the provided credentials are related to the exact user who claims to be.

Service Authentication: this use case is responsible to check whether the service is the exact one which the user wants to access or if the service is what it is claimed to be.

Connect others user´s computing devices**:** check the certain user's SSh and connect automatically the rest of the user's computing devices that are part of the SS. There is an option to send a list of the rest of the computing devices stored in the SSh in order to provide manual connection to the user. In that case, the user will choose which of his/her devices to be connected additionally in automated manner.

Connect non-user interface devices: check the certain user SSh and connect automatically the rest of the non-user interface devices, part of SSh related to the user.

Service Subsystem Part components:

Service Provider Manager: The component creates, manages and deletes thing's authorization and service connection within the IdM system.

Access Right Management*:* it specifies authorization making rules and performed actions based on identity information provided from IdPSP. The access rules are not discussed and investigated and are considered for out of scope of the thesis because they are specific in terms of implementation.

Thing Connection: defines the required order of messages for establishing thing-services connection.

Authorization Verification: action whereby SSP checks authorization of the certain thing to execute any operations with a service.

4.6.3. STSO IdM system structure

This section describes the structure of the proposed STSO IdM system. The visual presentation includes actors and relationship between them, represented by UML class-diagram, given in Figure 4.11.

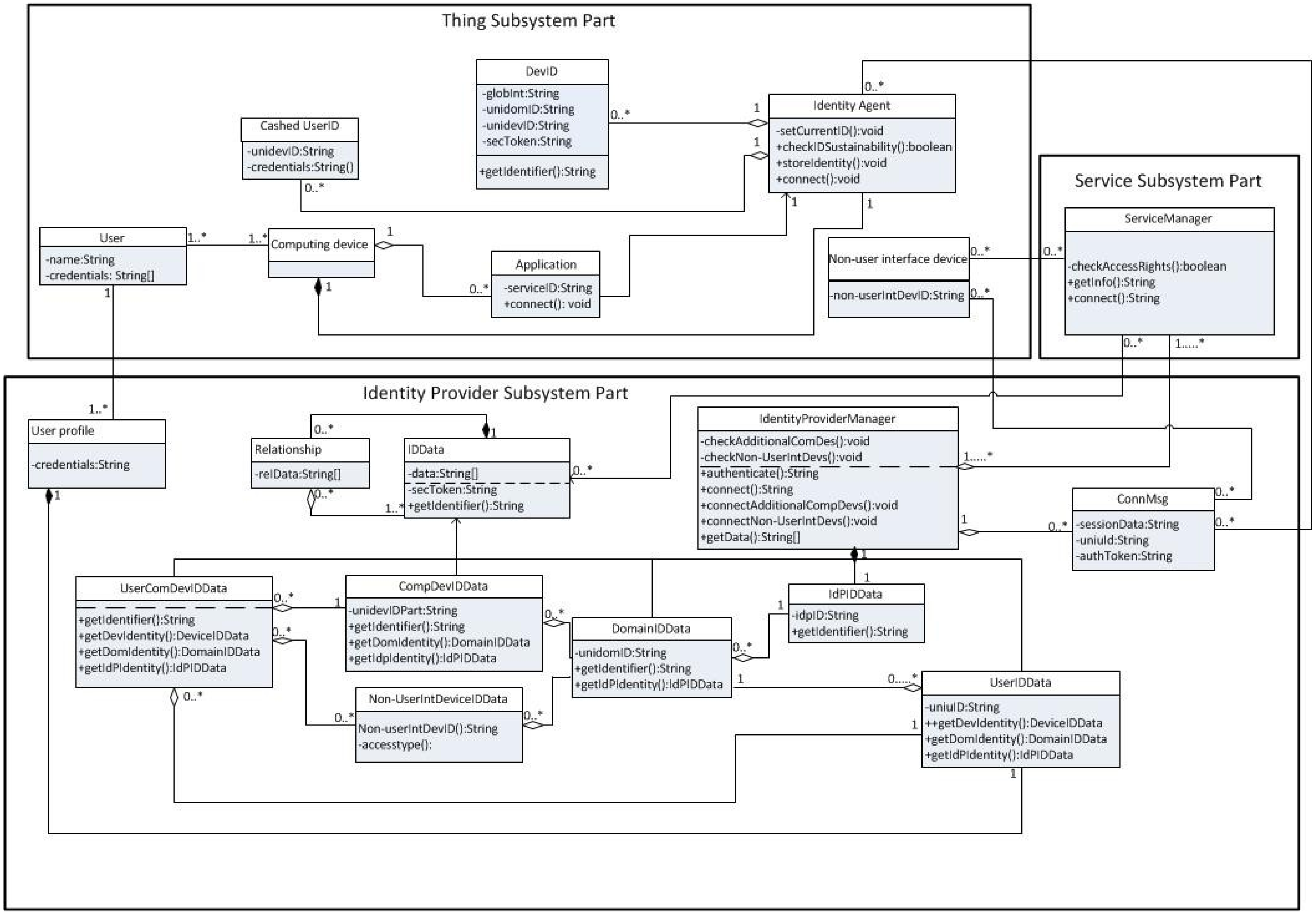


Figure 4.11 Class diagram of STSO IdM system

The main components of the system are TSP, IdPSP and SSP discussed already in the Section 4.6.1.1. As a matter of facts the system's design allows relationships "many-to-many" within various subsystems, and those links are given in the class diagram on Figure 4.11. Thus, the proposed IdM is considered as distributed and federated.

TSP is that part of the system which represented thing related information. It contains Identity Agent, part of the user's computing device and is responsible for providing authentication functionalities to the operating system and higher-level subsystems such as third-party applications. The computing device identities are stored in TSP.

TSP provides non-user interface device identity information, security token and domain related information to IdPSP in the communication process. The diagram shows also the Application class as a part of TSP. It is used to define the applications utilization of the system. As a requirement, it is necessary for the apps to use properly developed APIs - awarded from the system, invoking connection by Identity Agent and being compatible with services' identifiers which claims to access. The IdPSP component is responsible for providing identity data to the SSP. It works in collaboration with TSP. The data stored in IdPSP can be obtained and used only from trusted services which have pre-signed agreements with IdPSP. The trust mechanisms and agreements processes are not investigated and discussed in this thesis. One of the possible solutions for trusted service provider management is using of pre-stored list at the IdP containing service identifier and pre-wise secret. The collaboration between IdPSP and TSP is based on trust by providing security information. A certain security information implementation process is beyond the scope of this written document. As a possible solution is the usage of X.509 certificates and in particular - secret for Diffie-Hellman key exchange or pre-shared token.

SSP uses identity data related to user's devices (*dtype,unidevID*) to perform their authorization. SSP can be local or remote which depends on a certain service.

4.6.4. Main actions of the system

The main objective of the proposed IdM system is to enable service access by mechanisms for "thing" identification and authentication respectively using the information related to the current human user. The system functionality is based on STSO connection establishing procedure, involving authentication connection as a part of it. The latter one is presented separately in Section 4.6.4.2 in order to be clearly analyzed. Detailed explanation of STSO feature and performed actions by the things are presented in Section 4.6.4.1.

4.6.4.1. STSO connection

The general STSO connection procedure is consequent process of actions. Flow information messages involved in the STSO connection diagram are presented in Figure 4.12.

1. STSO connection diagram describes a case whereby a given computing device is utilized by a human user and the latter intends to connect local or remotely available service through a certain application. Moreover, the user may utilize beforehand applications which require automatic connection to the service, independently of user's intentions.

2. Application sends connect request to IdentityAgent providing service ID or alternative information related to requested service.

3. IdentityAgent uses the provided service information in order to establish communication with related ServiceManager and learn about IdPs relationships with the service and the required identity fields.

4. IdentityAgent obtains certain information associated to desired service from ServiceProviderManager

5. IdentityAgent checks whether the provided computing device identity is active (if there is any) and appropriate for the service by using IdP list related to the service.

6. Subsequently, IdentityAgent notifies the user about the required identity data fields and gives an option for identity switch based on service requirements

7. The diagram shows two alternative login ways. The first one is optional automated connection where all of the devices related to the user are automatically connected based on only one thing identification. If certain computing device(s) is(are) recognized by IdPs regarding user's preferences, STSO is activated.

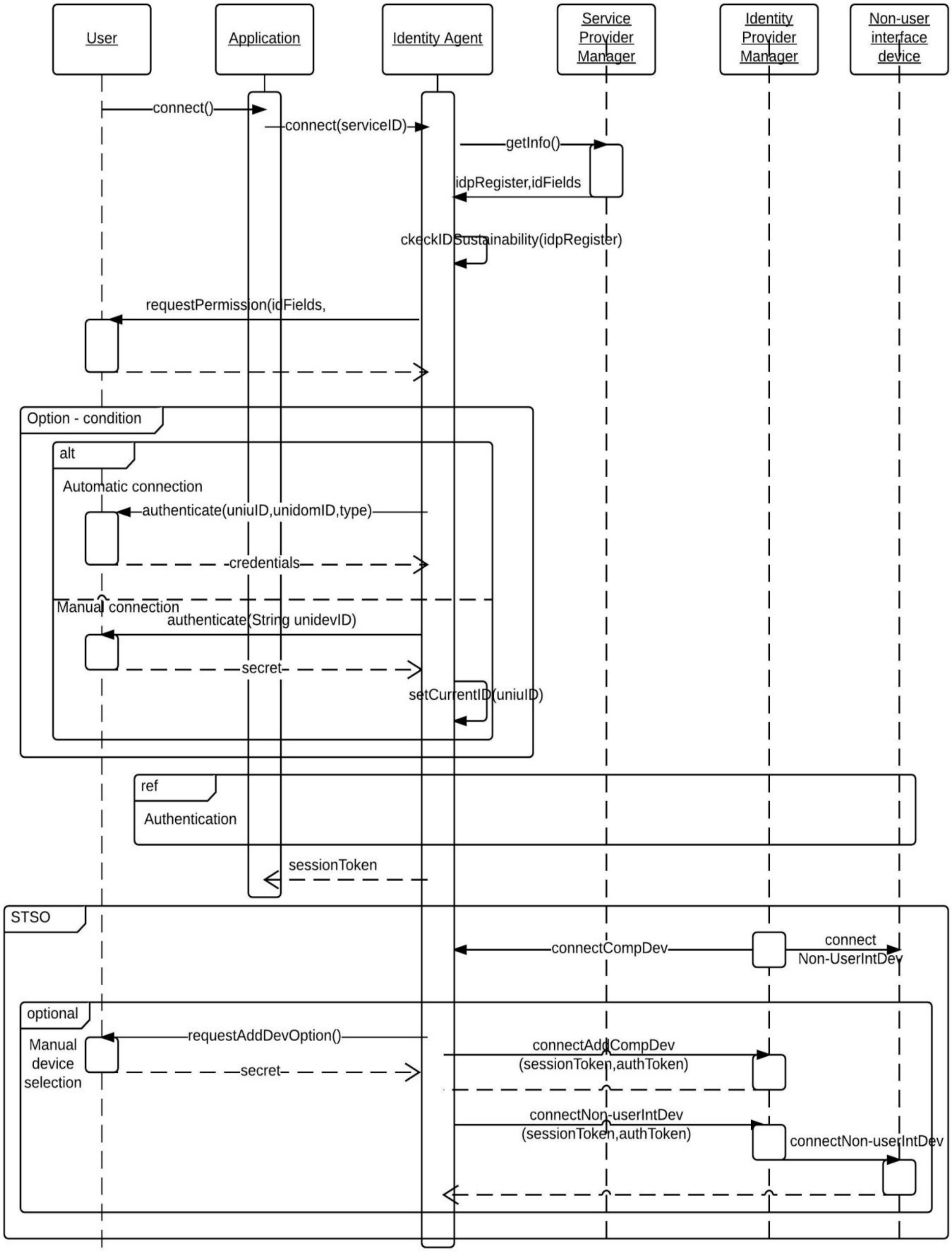


Figure 4.12 STSO connection sequence diagram

8. If the user wants manually to confirm his identity and choose device for utilization, the the manual connection option is available.

9. Then, the provided thing's credentials should be checked by IdentityAgent or IdP, and they are required parties in the authentication procedure. Next step in the diagram is the authentication which is further explained in Section 4.6.4.2.

When the authentication is successfully completed, sessionToken is being set from IdentityProviderManager and send to IdentityAgent. The latter sends a received sessionToken to the Application which needs that token in order to establish further own communication to the service without elaborating with Identity Agent.

Connection procedure includes STSO feature where the IdentityProviderManager sends connection device request to the both computing and non-user interface devices groups related to the current user profile. That allows automatic connection to other user related devices, after one of the things (user or computing device) is identified and connected. The procedure is enabled by recorded connection in the ConnMsg class managed by the IdentityManagerProvider.

Optionally, the user can choose manually devices which he/she would like to utilize.

- The IdentityAgent asks the user if he/she would like to access the service by utilizing other of his/her personal devices.
- The user might agree and choose some additional devices and specify a secret derived as an authToken. The latter will be used in the message send to the IdentityProviderManager later on.

The ServiceManagerProvider requests authentication from the IdentityProviderManager (Figure 4.13.), then:

- The IdentityAgent sends message to the IdentityProviderManager to request for connection to additional computing devices and non-user interface devices regarding the user's preferences. The message contains authToken and sessionToken.

- The IdentityManagerProvider receives the message for connecting additional devices, performs the authentication and sends a connection message to the targeted devices, if the authentication is successful.

4.6.4.2. Authentication

As it is mentioned above, the authentication sequence diagram is presented separately in Figure 4.8. The diagram includes some steps which are a part of the authorization, in order to find out and check the rights for using a certain service.

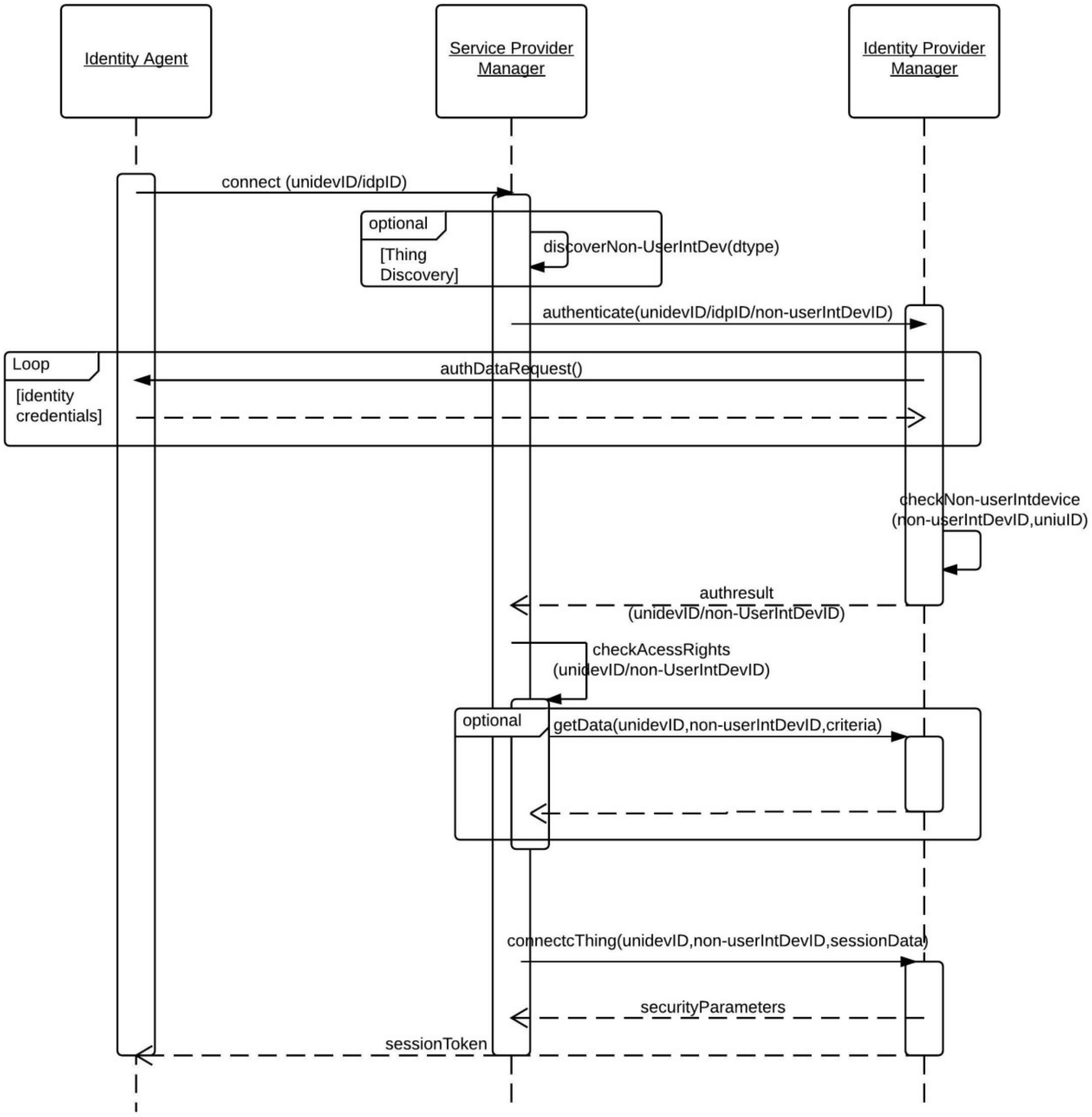

Identity Agent
Service Provider Manager
Identity Provider Manager
connect (unidevID/idpID)
optional
[Thing Discovery]
discoverNon-UserIntDev(dtype)
authenticate(unidevID/idpID/non-userIntDevID)
Loop
[identity credentials]
authDataRequest()
checkNon-userIntdevice (non-userIntDevID,uniuID)
authresult (unidevID/non-UserIntDevID)
checkAcessRights (unidevID/non-UserIntDevID)
optional
getData(unidevID,non-userIntDevID,criteria)
connectcThing(unidevID,non-userIntDevID,sessionData)
securityParameters
sessionToken

Figure 4.13 Authentication procedure sequence diagram

1. The beginning of the authentication procedure starts when the IdentityAgent contacts a ServiceProviderManager of a desired service by providing information about activated unidevID or idpID in order to be authenticating the proper device if the service has relations to more than one IdPs. The IdentityAgent sends connection request message to the ServiceProviderManager

2. The ServiceProviderManager checks and discovers which non-user interface devices (dtype) should be authenticated based on a specific service requirements and user preferences.

3. The ServiceProviderManager analyses the provided identifiers (unidevID/idpID), adds dtype if it is relevant after the thing discovery and sends request for devices authentication to the IdentityProviderManager.

4. The IdentityProviderManager sends request for identity-related information to the IdentityAgent, installed in the computing device because authentication is needed. The requests and responses in both ways are transferred directly or indirectly (forwarded by ServiceManager). In the process of implementation the accurate identity information, methods and techniques of messages transfer will be defined.

The IdentityProviderManager may check and verify if provided combination of identities related to a thing has a permission to use a certain service. If the access is not allowed, the authentication fails.

5. The IdentityProviderManager checks and verifies if non-user Interface devices can be used by a certain user based on providing combination of non-userIntDevID,uniuID. The IdentityProviderManager can also require ServicManager identification.

6. After successful device validation, the IdentityProviderManager sends authentication result message (udevID,non-userIntDevID) to the ServiceManager as a proof of user′s devices identity.

7. The ServiceManager executes own authentication procedure. It may require additional identity information to be provided by IdentityProviderManager linked to udevID,non-

userIntDevID. The implementation process will define the possible mechanisms for authorization.

8. If the authentication is successful, the ServiceManager sends request to the IdentityProviderManager to connect the service to authenticated computing and non-user interface devices.

The IdentityProviderManager serves to present the identity data to the services and devices and manage the communication between them.

9. The ServiceManager ensures secured communication by obtaining the security parameter.

10. The device receives the sessionToken containing the information for the device and service authentication, accessed identity data and security related information needed for communication.

4.7. Discussion

4.7.1. Technical discussion

This section presents a technical discussion based on requirements fulfillment, comparison between the proposed IdM and the reference IdMs, part of Section 4.1. That part also includes the IdM analysis based on the seven laws of IdM and STSO IdM realization in context of eWALL.

4.7.1.1. System requirements fulfillment

The proposed novel IdM user-centered system and its main STSO feature are fundamental for ensuring innovative way of automated identification. IdM proposal is based on the best existing techniques improved by novel identification algorithm through computing devices. The proposed STSO IdM system is analyzed by taking into consideration the discussed requirements for IdM in IoT (see Chapter III) and the end users' vision and perception about them.

In terms of flexibility, the STSO IdM offers identification by using all of the things in IoT by introducing the STSO feature. The system enables communication between computing and non-user interface devices in the network, used directly or indirectly by the user. Moreover, the

Identity Management in the system is cloud-based which is another premise and fundament for ensuring the scalability and mobility.

The proposed IdM is able to support various protocols in order to provide data information which might be in a different format such as JavaScript Object Notation (JSON), XML.

The system does not put limitations on the devices' type or vendor because of the proposed identifier format (see Chapter 3) as long as they are able to communicate with it over the provided for that purpose RESTful APIs and provides method for extensibility.

The system could theoretically be assessed as reliable due to its data flow model considerations for appropriate relations between the logical entities. The presumed use case scenarios consider system's STSO procedure failure or different user's preferences, and provide alternative mechanism for manual login and access to services. The lack of holistic system integration, functional testing and evaluation does not allow to claim the reliability requirements are met with full extend of certainty.

The system requires authentication of all operating within it devices thus the privacy of the data is among the main concerns for the IdM. The privacy support gives possibility for manual identity and device connection if a user requires that. The *Service Manager* controls the access rights to the system service and *Identity Manager* controls services rights by the identity data management policies for user identity creation, storage and deletion based on the proposed thing identifier format (*dtype*|*gloInt*|*locInt*|*unidomID*|*unidevID*|*uniuID*). The introduced by the author CDR algorithm is aiming to further improve the privacy. The CDR algorithm does not exclude the standard and most typical method for identification - username and password.

It is crucial that the IdM meets the user's' requirements otherwise there is a potential risk of failing of the system because of the lack of real users utilization. Analyzing the need of profile creation before system utilization that will not be an issue because the process is similar to the web-service profile creation. The advantage is that based on only one profile for STSO IdM, the user will be identified and be able to utilize various services by using different devices. Furthermore, the user will be able to define and manage his/her own rules in the stage of profile creation in terms of device connectivity (automatically or manually), services access, number of computing devices as an input data for CDR algorithm. The system design is expected to be user-friendly and will not require specific knowledge or trainings. It cannot be claimed that the system is completely user-friendly because of the lack of implementation and usability test investigation among users. The main STSO feature of the IdM enables automatic way of thing connection, and at the same time it provides and ensures directly or indirectly always responsive services because it provides seamless interconnectivity between computing and non-user interface devices.

4.7.1.2. *Comparison between the proposed IdM system to others IdMs in IoT*

Device-based system - Comparing the proposed STSO IdM with a typical device-based systems (see Section 4.1.) some similarities can be found because the strongest aspects was used as a fundamental basis for designing and proposing the STSO IdM system. The author's system is with increased complexity that includes authentication and reliable privacy and identity management. The possibility of thing's identification and the proposed STSO feature enables data exchange between all of the identified things in the system, including non - user interface devices is considered as a similarity with the device-based system - Cooltown.

In comparison to the ONS the STSO IdM enables device discovery and identity data management (acquisition, storage and deletion). The proposed system in the thesis focuses on human end-user and his/her devices no matter the driving technology, distinguished from ONS device metadata management techniques.

User-oriented system - The STSO is a user-centered system, which combines user and device identity and this identity is managed by included in the architecture *IdentityManagerProvider*. In order to provide independent transmission of messages the computing devices utilizes embedded software components. Additionally, in IdPSP users' profile contain information regarding non-user interface device. The STSO feature and the CDR algorithm extend IdM capabilities to search and find things, and distinguish users based on pre-defined agreements. STSO system goes beyond the user-interface web-based access to services.

Similar to OpenID, STSO IdM enables multiple identity storage related to the user in IdPSP and selection of one or more identities. The identity process is more automated and the entire identity data is provided after service authentication. Looking into SAML, the first similarity is clearly appealing - enabled federated IdM. SAML operates with SSO on a web level, where STSO IdM enables single thing sing on the whole “thing” level in IoT which is on the other hand is similar to OAuth2. The required pre-communication relationship establishment between the parties is also a present in the both user-oriented systems. The third similarity is the authorization mechanism for access control to the system’ resources - for STSO this is the identity data and services. In terms of identity management and authentication, STSO is most similar to OpenID Connect. Looking at MAGNET and STSO IdM, the similarity appears into the personalized user profile and the service-oriented characteristics of the both systems. The proposed by Paraktish IdM is similar to STSO because both of them are based on context identity for things but the human-user is not involved as a main part of the IdM. IdM Mobile Health and STSO address shared and non-user interface device relations. Similar to proposed SDSO whether only computing device are addressed, STSO proposes a collaboration and interaction between all the things in IoT. In addition, the used identifier format in STSO includes *device type* which is significant in communication process within the heterogeneous networks.

4.7.1.3. Seven laws of Identity

Meeting the law’s requirements is crucial no for evaluation and assessment of the system. In that way, taking into consideration the ‘Seven laws of Identity’ defined by Cameron [47] ,the system is being analyzed, in terms of the user’s privacy as important factor when his/her identities are required for accessing web-service.

1.User control and consent - “Technical identity systems must only reveal information identifying a user with the user’s consent.”

The first point of the law in STSO IdM system is addressed by giving awareness of the user about admissible identities and identity data before and during the login phase, provided by IdPSP-SP collaboration.

2.Minimal disclosure for constrained use

‘The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.’

STSO meets this point by limited providing of identity data (*uniuID*) before service to be authenticated. In addition, IdPSP might inform the 'thing' (user, device) for needed identity data requests by the certain service. *ServiceProviderManager* controls the service identity and does not allow identity sharing between different services.

3.Justifiable Parties

"Digital identity systems must be designed so the disclosure of identifying information is limited to parties having necessary and justifiable place in a given identity relationship."

By performing 'thing' and service authentication, the proposed STSO IdM system meets Justifiable parties requirement. The identity data is available only after authentication procedure is successfully performed, based on Identity and *ServiceManagerProviders*.

4.Directed Identity

"A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles."

The partial device identifier (*unidevID*), the provisioning of *gloInt* and *otype* can be used in the process of private or public thing discovery, thus the system support Directed Identity.

5.Pluralism of Operators and Technologies

"A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers."

The lack of investigation for the collaboration between multiple IdPs does not allow STSO IdM to meet this law requirement. From user's perspective, he/she might use and takes advantages from various IdPs regardless the technological solutions behind them.

6.Human Integration

"The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks."

Involving the human-user as a main part of the system by giving him/her the possibilities for managing and creating rules in the system, and being part of the communication directly or indirectly is one of the goals. Proposing a CDR identification algorithm also aims to protect and minimize any identity attacks. Stating the above, and considering the identification and authentication mechanisms as a part of the system, are an evidence that the STSO IdM meets this point.

7.Consistent Experience Across Contexts

"The unifying metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies."

By involving domains context usage, STSO enables thing recognitions thus the system meets this requirement.

4.7.1.4. Implementation

The STSO system can be considered as a novel promising solution for identity management in IoT on theory but the next phase of real software and device implementation and testing is crucial to assess and analyze the device's and user's behavior and system performance. In the process of implementation, the components or parties which are not addressed in the thesis should be covered by using appropriate solutions. The prototype development and implementation should not emphasize significant problems because for most of those aspects an optional solution is proposed by the author. The features set of the proposed STSO system depends on other ICT technologies providing: heterogeneous networks communication, dedicated software artefacts and functionalities, security policies, data storage, etc. This means that information collaboration model and between multiple parties is needed. There are some functional and logical components (referred as "Delimitation" in Chapter 1) beyond the scope of the thesis which means the design is open for various technological implementations and further development.

4.7.1.5. STSO IdM in context of eWALL

Referring to proper and meaningful scenarios for implementation of STSO IdM, good examples are the e-Health and, in particular, the Ambient Assisted Living (AAL) services. On one hand, when talking about personal health related data, the security and the privacy issues are raised and using a proper IdM and user profiling solutions, in this scenario, is crucial. On the other hand, when elderly or cognitive impaired personas are supposed to benefit from modern AmI solutions for independent living, the question for the ease of use and the level of adoption of such system is still open. Privacy and security supportive technologies like the proposed from the author STSO IdM and CDR algorithm for authentication have the potential to fill in this gap for proper technology solutions.

As a proof of the proposed STSO IdM system concept, its realization and usage in context of the eWALL project is discussed below.

eWALL is an intelligent AAL platform that incorporates a myriad of wireless and wired communication and data processing technologies and networked devices that interoperate in the frames of it in order to provide e-Health services [48].

The European-funded under Framework Program Seven (FP7) project eWALL (eWall, 2013) proposed an affordable, easy-to-implement, smart, cognitive environment that "senses" and "learns" the needs of the user who lives in his/her house and provides unobtrusive daily activities and healthcare support [48].

The eWall project identifies and addresses, among others, the a number of generic system and user requirements (given in Table 4.1. and Table 4.2. respectively), which are relevant to the proposed STSO IdM.

Table 4.1 Some of the generic system requirements in eWALL [49]

	Description
Flexibility	Ability to support a variety of market available or eWALL developed user and network devices.
Compatibility	Ability to integrate various information from various devices in a user transparent manner.
Responsiveness	Ability to dynamically react and/or reconfigure eWALL platform elements.
Security	Ability to secure the eWALL users' data from obtrusive and accidental eavesdropping.
Privacy	Ability to keep personal information from being disclosed and shared with unauthorized parties.
Service orientation	Ability of a system to ensure reusability and composability of services and service components.

Table 4.2 Some of the generic user requirements in eWALL [49]

Goal	Description
Usability	eWALL is easy to use.
User experience	eWALL is pleasant to use.
Personalization	eWALL can be personalized according to aesthetics, preferences and habits of the end-users.
Unobtrusiveness	eWALL is unobtrusive.
Minimum user input	eWALL requires the minimum possible input from the user.

The key requirements for enabling a sustainable AAL system are the personalization and adaptation to specific user needs and preferences, the resourceful data and context sharing between the different required services. This includes: the handling of multiuser identification, auto configuration and calibration systems. These requirements require highly personalized usability and unobtrusive environment and vital signs sensing [49].

The eWALL system is composed of two main subsystems: the eWALL Sensing Environment and the eWALL Cloud where the interaction between the two is given in Figure 4.14.

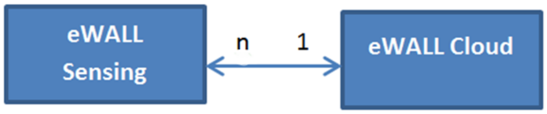


Figure 4.14 eWALL main subsystems [49]

The *eWALL Sensing Environment* is deployed over a physical space and interacts with the primary user. In that sense there are two types of sensing environment: 1) Home Sensing Environment, operating in the physical surroundings of the user, when he/she is at home. It monitors the status of environmental parameter such as humidity, temperature, luminosity, motion etc. 2) Mobile Sensing Environment is operating around the user is even if he is outside of his/her ambient environment. The data from the wearable devices is transferred to the home device gateway wirelessly when the user is within the communication range of it. Such wearables could be smartphones, pulse and blood oxygen saturation sensors, body temperature sensors, ect.

The *eWall Cloud* – the data processing and storage in eWALL are ensured by the eALL Cloud connected with the home environment of each user. eWALL applications are available and driven based on so the called “service bricks” components and they forma the pool of various eWALL cloud services. The applications use JSON/RESTful data format over HTTP communication protocol.

These environment and biometric sensing technologies, alongside with their cloud based orchestration core, lack of better utilization of resources in terms of the need for deployment of private sensor nodes for every user. In the particular example with eWALL each user can benefit only from his own environmental sensors. The presence of multiple eWALL users in a single sensing environment is not envisioned within the project, because of the absence of devices and users scheme for IdM, which to allow real time user and device recognition.

STSO IdM in eWALL

Use case: eWALL platform envisions interaction with the users in their homes or outside of it. The system does not describe a scenario for user roaming between different eWALL environments, for example if two users of eWALL are being present in a single sensing environment (i.e. simultaneous usage of the home sensing environment devices by two different users).

As a cross point between eWALL use case scenario and the STSO IdM, the use case described in Chapter 2, Section 2.3 can be referred and analyzed. Similar to the STSO IdM user Charlene, any eWALL user (for example Bob) can benefit from automated identification algorithm based on his computing devices, in context of eWall mobile devices. When Bob visits his family home, hospital or activity center, he will be able to access seamlessly and use in automated manner all of the eWALL applications by using STSO, no matter that he is not at his own home environment.

eWALL improvement by using STSO IdM

In order to improve the eWALL user identification and to provide mobility and responsive eWALL applications, the eWALL project concept could be extended with implementation of STSO IdM subsystems components included in the architecture as given in Figure 4.15

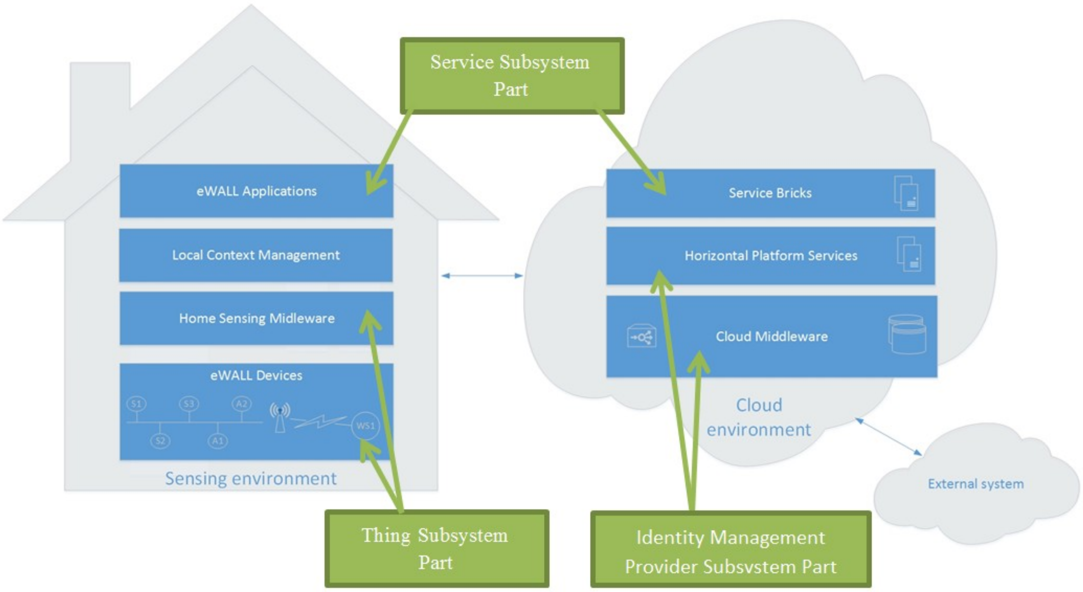


Figure 4.15 Implementation of STSO IdM subsystem parts in eWALL

TSP resides on the eWALL devices and Home Sensing Middleware components of eWALL where the eWALL users, sensors and computing devices could be assumed as part of the infrastructure, when referring to IoT and IdM. The Identity Agent should be installed on the eWALL primary user's computing devices, in order to enable the STSO feature.

IdPSP should be deployed on the Cloud Middleware and will become a part of the Horizontal Platform Services where the user profile information in eWall is stored and managed at a cloud level. The IdentityManagerProvider should be implemented on a cloud middleware level in eWALL to enable identity functionalities such as thing identity creation, management and deletion. What is missing for the eWALL system on a cloud level is device identity management related to a certain user.

SSP is already represented in eWALL by User profiling functionalities the respective applications and services assignment to a certain user.

The implementation of the STSO IdM within eWALL will affect the discussed above building blocks and should be included as a part of the holistic architecture of the platform, since the IdM is not a single component or plug in. There should be dedicated C++ components on a DeviceGateway level and other Java software artefacts deployed on a cloud level. The implementation may also cause changes in the JSON data format used for the sensors and actuators data representation and exchange, as well as it will require storing of additional device identity data both on the homePC (CouchDB) and eWALL cloud (MongoDB) databases.

By introducing and implementing the *IdentityAgen*t and *IdentityProvider*, eWALL will be able to offer the functionalities of the CDR algorithm where the user input efforts will be minimized. The password retyping and remembering will be substituted by the algorithm, which will contribute for simplifying the system and improving the privacy and security.

A number of advantages should be summarized as follows:

- CDR algorithm will improve the eWALL system in terms of usability and ease of use. It also is a way of performing better user experience, improved personalization and minimizing the need of user input which is important from senior or cognitive impaired users' point of view.
- STSO IdM will improve the eWALL system in terms of mobility and inner system sites roaming – by ensuring user identification and eWALL application access.
- STSO will add value to the eWALL system by providing Service orientation and ensuring always responsive services
- Personalization and privacy of services by improved ability for the user to create the rules for identification within the eWALL system.
- STSO IdM and CDR algorithm will improve the security by reducing the possibility for personal data abuse or unwanted system intrusion.

With introducing the STSO IdM in eWALL both the users and the business parties will benefit from better utilized sensing infrastructure, seamless roaming between eWALL sensing environments, improved personalization and security of the services and better monitoring of the patients.

4.7.2. Business case analysis

The business analysis of the system includes summarizing and discussing the most significant values of the system from business point of view. Market analysis, market share or any kind of surveys are out of the scope of the analysis due to limited time resource.

Similar to the user and system, the business has its requirements as well. Some of those requirements are similar or same with the user´s ones. If the offered services or applications do not meet the expectations for interaction and usage, they will not be useful and meaningful for the users, which will lead to reduced or absence of market for that kind of services. Additionally, the business has a mandatory requirement to implement and offer profitable, added value and providing user-experience services.

The following factors are identified as essential for successful business models involving the latest IoT trends [50]:

- ***Real-time data and analysis:*** The business models should be designed to accelerate data capturing and analyzing operations in order to process data from diverse data centers, assemble, analyze and deliver results in real-time

- ***Intelligent operations:*** IoT industry needs to involve intelligent operations to control data from diverse end points

- ***Diverse revenue streams:*** The IoT business models should be created to produce novel services, software and devices in extending the existing products in order to generate new revenue sources

- ***Turn on and turn off features:*** other cornerstone of building IoT business models is the feature of turning off and on in diverse orders and getting additional values of devices and committed software for those devices.

From a business' perspective, the IdM provides tools for simplifying the process of user identification and uncovers Blue Ocean for plenty of disruptive services and applications in almost any business aspect which involves ICT. As a consequence, the usage of the proposed IdM system will add value to a number of currently used services by giving them intelligence, personalization and context-awareness. The model is a basis for development and creating new security access, privacy management and user-centered or similar IoT applications.

Values and competitive advantages of the STSO system

- Reducing the manual use of passwords - respectively that means the easier way to the users for utilizing services which have agreements with IdM
- Possible service/application identity management based on computing and non-user interface devices only
- Time-saving process - automatically identification and STSO feature providing
- Effort saving process by introducing STSO feature and novel algorithm for user identification based on computing device recognition
- Always responsive services no matter time and place
- User-centered applications services
- Context-aware applications.

After successful real implementation and testing, the proposed IdM system can be integrated in various fields which among others are:

- Personalized e-Health and e-Wellness application (hospitals, pharmacy etc)
- Enterprises - for access purposes for instance
- Shops - to reduce the queues by automatic recognition of the user and using his/her bank information for payment
- Smart transportation services.

IoT significantly increases the number of security risks that the business and the consumers will face, since any device connected to the Internet which has an embedded operating system is potential backdoor for the attackers. Some of the critical IoT enterprise risks to be taken in to consideration are listed as follows [51]:

- ***Disruption and denial-of-services attack*** - leading to operational failures and interruption to the enterprise or private level services.
- ***Misunderstanding the complexity of vulnerabilities*** - to understand where the vulnerabilities fall on the complexity meter, and what threats they pose.

- ***Security analytics capabilities*** - to be able to detect malicious activity and improve the service responsibility offered to the users
- ***Lack of modular hardware and software components*** – being able to isolate any device or software components which are being compromised by attackers.
- ***Redundancy failure*** – if any component fails another should be there to take over its place.
- ***Lack of bandwidth*** – if due to any reason critical applications do not receive their required bandwidth, consumers will have bad experiences.

Enterprises and business parties should have responsive attitude toward the implementation of best security practices when dealing with IoT. Threat modeling will be necessary in order to ensure the security, confidentiality, integrity and availability, both on a user or enterprise level.

The main principle of the system, STSO feature can be used in the future ICT solutions and be a part of successful business models providing business intelligence and having potential to be a disruptive technology. The open design of the system classifies it as such with future potential for development and integration of novel features thus to be a stage of the evolution of IoT to Internet of People and Everything.

4.8. Identity Management Systems summary

The usage of different devices, protocols for communication, software characteristics and security mechanisms are a solid challenge which IdM system faces and should balance to provides its features and ensure responsive services. In this chapter, the Identity Management system definition and currently existing IdM systems were presented. Also, the system and user requirements have been identified. In this chapter, introduction of concept for IdM system addressed "thing" identity management using only one thing sign on identity was proposed. The description of the main functionalities and actions in the system such as STSO connection and authentication of computing and non-user interface devices were presented. The evolution of the proposed STSO IdM from technical and business point of view were discussed in order to identify the advantages of the system and find out future research fields.

Chapter 5

Conclusions and future work

This chapter concludes the thesis and proposes future aspects for research, based on the proposed ideas and the theoretical analysis which was done in order to validate and proof of the proposed concepts. The thesis addresses the IdM issues in IoT and proposes STSO identity management system, identifier format and user identification algorithm.

5.1. Summary of Contributions

The presented thesis identified some of the important challenges for IdM in IoT. The thesis proposed an extended and different vision for identity management that enables automated communication between various things in IoT which is time and effort saving for the end user. Also, it ensures providing and offering always responsive services to the users. The introduced STSO IdM system is a novel solution addressing the communication and interactions between all of the things involved in IoT in automated manner thanks to the proposed identifier format. The STSO feature serves the possibility of accessing services through only one thing (no matter human user or device) sign on to identification without any need of separate identification on web level or any additional actions (synchronization of wearable devices etc). The proposed CDR identification algorithm ensures automated user identification and addressed privacy and security issues and prevent from attacks such as password guessing or SSO web feature when the shared devices are used.

In the Chapter 1, the problem was identified and the motivation to solve it was discussed. Furthermore, the goals and objectives of the thesis' research were clarified. The research workflow and methodology of the thesis were presented.

In the Chapter 2, real scenario use cases were given in order to understand the challenges and requirements for use identification. To address the identity issue, CDR algorithm based on computing device recognition is proposed in order to solve the problem in automated, easier and secured way. The identification rate of computing device coefficient was proposed for assessment of the algorithm.

In the Chapter 3, the research challenges were identified based on identification schemes literature review. Then, the introduction of an identifier format addressed identity management issue in terms of mobility, scalability and thing type was presented.

In the Chapter 4, a concept for IdM system that addresses identity management of the "thing" based on only one thing sign on identity was proposed. The main functionalities and actions in the system such as STSO connection and authentication of computing and non-user interface devices were described. Theoretical analysis of the proposed STSO IdM from technical and business aspects was discussed in order to analyze and proof the concept.

Finally, in the last chapter the contribution of the thesis is summarized and presented. The aspects which were not considered in the thesis are given to be further explored and investigated.

5.2. Conclusion

The number of devices has been only and rapidly increased and it is predictable that this trend will continue in the next years. This means only one - billion of connected devices, requiring automatic and secured processing will be deployed and operating. The evolution of the ICT industry will trigger new disruptive technologies that will be fundamental and will indicate the need of new business services and applications models, massive “thing” communication capacity, next generation infrastructure, integration of mass-scale cloud architecture and easiest way of action performing ensuring full control from user's perspective.

As an output of the thesis, the proposed STSO IdM is among the first in IoT to addresses thing identification by device-based user identification (CDR algorithm) and user/device-based device-to-device communication (STSO feature) and multiple thing connection. The proposed attractive user-centered solution aims to takes the attention towards thing related communication involving the human user as an active player in the system. The user’s role and the proposed system functionalities are meaningful in terms of IdM. Therefore the proposed system will contribute for the evolution of the Internet towards being part of Internet of People and Internet of Everything. It is a matter of high possibility that the future ICT will experience the existence of industry and regular user-oriented services and applications in order to provide context-aware and user centric services.

5.3. Future work

5.3.1. Feasibility stage

Although the theoretical analysis of the STSO IdM is considered as a promising, the system must be implemented and tested in a real practical situation, and then the same tests and examinations should be performed in a real network scenario. The reasons why feasibility stage is mandatory are obvious but the main benefit is that the human user involved in the process could provide detailed feedback about user creation, identification, concept and friendliness of the system, responsiveness of services, etc. Furthermore, during that stage various options addressing out-of the scope aspects and their elaboration and deployment can be tested. The implementation of proposed by the author CDR algorithm as a part of the system should be also tested in order to ensure that it identifies the human users in a right manner, it has to have the best performance. Moreover, the algorithm could be additionally extended by adding thing behavior pattern for user identification, e.g. using BETaaS gateway [52]. Summarizing the mentioned information, the feasibility stage could define more fields for further development of the system.

5.3.2. RESTful API

A RESTful API for interaction between third party apps and computing and non-user interface devices is not elaborated. API specification defining is important because it will enable quick technology learning and its using in the services and applications development. In addition it will ensure interoperability and integrity of the system.

5.3.3. Survey

One of the most common methods for gathering users' feedback and concerns is performed by surveys, regarding various business and technical issues.

From a technical aspect, users' concerns about their privacy, when personal information is provided, is always sensitive field which could be a reason for unwillingness of using the system. Thus, holistic usability evaluation and survey regarding the usage of STSO IdM, e.g. IdPSP cloud or private deployment, personal and public sensors networks, has to be done involving different parties such as real human users of the system, identity managers, application and service providers or developers.

Concerning the business aspect, the system is considered for a value-added component within technological and service model components. Therefore, a holistic usability tests and user survey should be conducted to redefine the user-friendliness of the system and the time- and effort saving features. The mainly involved parties are: the real human users of the system, application providers and developers, service providers and developers, innovative-thinking entrepreneurs.

References

[1] "The internet of things" [Online]. Available: http://www.iot-i.eu/iot/public/news/resources/TheThingsintheInternetofThings_SH.pdf. [Accessed: 31-Mar-2015].

[2] K. Ashton "That 'Internet of Things' Thing - RFID Journal." [Online]. Available: http://www.rfidjournal.com/articles/view?4986. [Accessed: 31-Mar-2015].

[3] Jeroen van den Hoven, "Fact sheet- Ethics Subgroup IoT - Version 4.0." [Online]. Available: http://www.ethicsinside.eu/contact. [Accessed: 31-Mar-2015].

[4] M. V. Moreno, J. L. H. Ramos, and A. F. Skarmeta, "User role in IoT-based systems," 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 141–146.

[5] "Internet of People: Technology 2015-2025: IDTechEx." [Online]. Available: http://www.idtechex.com/research/reports/internet-of-people-technology-2015-2025-000388.asp. [Accessed: 31-Mar-2015].

[6] Ingo Friese, "Concepts of Identity within the Internet of Things - DG - Identities of Things - Kantara Initiative." [Online]. Available: http://kantarainitiative.org/confluence/display/IDoT/Concepts+of+Identity+within+the+Internet+of+Things. [Accessed: Apr-2015].

[7] Finjan Software Inc, "User Identification and Authentication." 2008. [Online]. Available https://www3.trustwave.com/software/secure_web_gateway/manuals/9.2.0/User_Identification_and_Authentication.pdf

[8] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497–1516, Sep. 2012.

[9] P. Mahalle, N. R. Prasad, and R. Prasad, "Identity Management Framework towards Internet of Things. CTIF Aalborg, November 2013

[10] "Liberty Alliance." [Online]. Available: http://www.projectliberty.org/. [Accessed: 03-Apr-2015].

[11] "Final: OpenID Authentication 2.0 - Final." [Online]. Available: http://openid.net/specs/openid-authentication-2_0.html. [Accessed: 03-Mar-2015].

[12] M. Weiser, "The computer for the 21 st century," *ACM SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 3, no. 3, pp. 3–11, Jul. 1999.

[13] B. Ndibanje, H.-J. Lee, and S.-G. Lee, "Security Analysis and Improvements of Authentication and Access Control in the Internet of Things," *Sensors*, vol. 14, no. 8, pp. 14786–14805, Aug. 2014.

[14] Dave Evans, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything." Apr-2011. [Online]. Available www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf [Accessed: November-2014].

[15] R. Prasad, Ed., *My personal Adaptive Global NET (MAGNET)*. Dordrecht: Springer Netherlands, 2010.

[16] Signals and Systems Telecom, "The Wireless M2M & IoT Bible: 2014 – 2020 - Opportunities, Challenges, Strategies, Industry Verticals and Forecasts." May-2014.

[17] "M2M: Machine to Machine and The Internet of Things trends | M2M trends, IoT Trends, Automation, Telemetry and Remote Monitoring." [Online]. Available: http://m2m.orangeom.com/. [Accessed: Mar-2015].

[18] O. Vermesan and P. Friess, *Internet of things: converging technologies for smart environments and integrated ecosystems*. 2013.

[19] D. Todorov, *Mechanics of User Identification and Authentication: Fundamentals of Identity Management*. CRC Press, 2007.

[20] ACM Workshop on Digital Identity Management, *Establishing and protecting digital identity in federation systems*. New York, N.Y: Association for Computing Machinery, 2005.

[21] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," 2012, pp. 553–567.

[22] M. Boatwright and X. Luo, "What do we know about biometrics authentication?," InfoSecCD '07 Proceedings of the 4th annual conference on Information security curriculum development, 2007, NY.

[23] M. D. Corner and B. D. Noble, "Protecting applications with transient authentication," MobiSys '03 Proceedings of the 1st international conference on Mobile systems, applications and services 2003, pp. 57–70.

[24] A. De Luca, E. von Zezschwitz, N. D. H. Nguyen, M.-E. Maurer, E. Rubegni, M. P. Scipioni, and M. Langheinrich, "Back-of-device authentication on smartphones," 2013, p. 2389.

[25] C. Feher, Y. Elovici, R. Moskovitch, L. Rokach, and A. Schclar, "User identity verification via mouse dynamics," *Inf.* Sci '13 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems., vol. 201, pp. 19–36, Oct. 2012.

[26] N. Aboudagga, M. T. Refaei, M. Eltoweissy, L. A. DaSilva, and J.-J. Quisquater, "Authentication protocols for ad hoc networks: taxonomy and research issues," Q2SWinet '05 Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks 2005, p. 96-104

[27] D. Rotondi and S. Piccione, "Managing Access Control for Things: A Capability Based Approach," in Proceedings of the 7th International Conference on Body Area Networks, ICST, Brussels, Belgium, Belgium, 2012, pp. 263–268.

[28] J. Song, A. Kunz, M. Schmidt, and P. Szczytowski, "Connecting and Managing M2M Devices in the Future Internet," Mob. Netw. Appl., vol. 19, no. 1, pp. 4–17, Feb. 2014.

[29] European Telecommunications Standards Institute, "Machine-to-Machine communications (M2M); Functional architecture." 2013. [Online]. Available: http://www.etsi.org/technologies-clusters/technologies/m2m

[30] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "PAuthKey: A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications," *Int. J.* Distrib. Sens. Netw., vol. 2014, p. e357430, Jul. 2014.

[31] J. Cubo, A. Nieto, and E. Pimentel, "A Cloud-Based Internet of Things Platform for Ambient Assisted Living," Sensors, vol. 14, no. 8, pp. 14070–14105, Aug. 2014.

[32] EU Framework7, Project, "RFID and the Inclusive Model for the Internet of Things." 2009, pp.43-54

[33] Anders Fongen, "Architecture Patterns for a Ubiquitous Identity Management System," The Sixth International Conference on Systems, 2011.

[34] C. Hu, J. Zhang, and Q. Wen, "An identity-based personal location system with protected privacy in IOT," Broadband Network and Multimedia Technology (IC-BNMT), 2011 4th IEEE International Conference on 2011, pp. 192–195.

[35] J. K. Siniša Srbljić, "Security of Web Level User Identity Management." [Online]. Available:

https://bib.irb.hr/datoteka/414370.02_1244_F.pdf [Accessed: Feb -2015].

[36] EU Project “IoT@Work WP 2 – COMMUNICATION NETWORKS D2.1 – IOT ADDRESSING SCHEMES APPLIED TO MANUFACTURING.” 2011. [Online]. Available: https://www.iot-at-work.eu/

[37] G. Roussos and P. Chartier, “Scalable ID/Locator Resolution for the IoT,” Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing 2011, pp. 58–66.

[38] “IBM Education Assistant video,” 01-Jan-2013. [Online]. Available: http://www-01.ibm.com/support/knowledgecenter/api/content/nl/en-us/websphere_iea/com.ibm.iea.was_v7/was/7.0.0.23/Security/SAML_Web_SSO/player.html. [Accessed: Jan-2015].

[39] Security Assertion Markup Language (SAML) V2.0 Technical Overview, [Online]. Available: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html [Accessed: Jan-2015].

[40] “Comparison of OpenID Connect with OAuth2.0 & SAML2.0,” *API Crazy*. [Online]. Available: http://apicrazy.com/2014/07/23/comparison-of-openid-connect-with-oauth2-0-saml2-0/.[Accessed: Jan-2015].

[41] “RFC 6749 - The OAuth 2.0 Authorization Framework.” [Online]. Available:

https://tools.ietf.org/html/rfc6749 [Accessed: Feb-2015].

[42] “OpenID Connect | OpenID.” http://openid.net/ .

[43] “oneM2M.” http://www.onem2m.org/

[44] C. C. Abdullahi Arabo, “Identity Management in the Internet of Things: the Role of MANETs for Healthcare,” Computer Science and Information Technology 1(2): 73-81, 2013.

[45] D. van Thuan, P. Butkus, and D. van Thanh, “A User Centric Identity Management for Internet of Things,” IT Convergence and Security (ICITCS), 2014 International Conference on 2014, pp. 1–4.

[46] P. B. Professor Do van Thanh, “Identity Management in M2M Networks,” 2014.

[47] “7 Laws of Identity | Kim Cameron’s Identity Weblog.” [Online]. Available: https://www.identityblog.com/?p=1065.

[48] EU Project eWALL http://ewallproject.eu/

[49] EU FP7 eWALL project, Deliverable D2.1, Preliminary User and System Requirements v1.0, February 2014

[50] "New Business Models Required for Internet of Things"[Online]. Available: http://www.iottechworld.com/business/new-business-models-required-for-internet-of-things.html [Accessed: May-2015].

[51] "Internet of Things (IOT): Seven enterprise risks to consider". [Online]. Available: http://searchsecurity.techtarget.com/tip/Internet-of-Things-IOT-Seven-enterprise-risks-to-consider [Accessed: May-2015].

[52] “BETaaS - Community.” [Online]. Available: http://www.betaas.eu/description.html#.VWtvjM-qqkp. [Accessed: May-2015].