A Distributed Identity Handling Approach Enriched with Identity Semantics

Mohammad M. R. Chowdhury
UniK-University Graduate Center
Post Box. 70, 2007 Kjeller, Norway
mohammad@unik.no

Josef Noll
UniK-University Graduate Center
Post Box. 70, 2007 Kjeller, Norway
josef@unik.no

Abstract

People rely on many forms of identities to access offline and online services. The inconvenience of possessing and using identities creates significant security vulnerability. This paper proposes an identity handling mechanism enriched with identity semantics which is believed to ease and secure identity usage. In this regard, user's identities are classified into personal, corporate and social identities, and they are going to be distributed over user's personal device and a secure network place. Corporate and social identities are represented through user's roles and relationships exploiting Web Ontology Language. Secure service access is ensured through multi-factor authentication method. Access is further restricted through authorization making use of user's defined roles and relationships. This paper demonstrates an implementation of service access by means of authentication and authorization through one's personal and corporate or social identities. The proposed solution is analyzed and compared with other relevant concepts, methods and solutions.

Keywords: authentication, authorization, identity, ontology, role, relationship

1. Introduction

Identification is a process through which a system ascertains the identity of a person who is trying to gain access to the system. It is essential to provide access to various value added services. Human beings play different roles while interacting with these services. Paper-based identities cannot be used while accessing services in the digital world. Moreover, different types of services require different types and forms of identities. People increasingly use computers to do business over the Internet. But accessing online value added services invariably requires typing various usernames and passwords for identification. These passwords can be captured and reused by hostile parties. To make the service access simple, hassle-free and above all secure, a manageable but usable identity mechanism is expected.

Mobile phone penetration is expected to reach 100% in most of the European countries[1]. It has become a foremost electronic device for worldwide communication because of its mobility, seamless and secure access provision to networks. In addition to this, mobile phone has always online functionality. Lately, computing capabilities of the mobile devices are enhanced manifold. Nowadays, there are provisions for being connected with the Internet using SIM from the laptop computers. It is evident that ubiquitous access and pervasive computing facilitate service access anywhere, anytime. In this paper, we focus on accessing the Web services through Mobile Phone/SIM card authentication.

User's identity data is not merely 'Information'. The semantics of identity information and the data itself are crucial for decision making, such as deriving access authorization decisions. This paper extends such interpretation towards an identity handling mechanism. In this regard, user's identities are classified into personal, corporate and social identities, and they are going to be distributed over user's personal device and a secure network place. User's roles and relationships represent a part of the corporate and social identities exploiting Web Ontology Language (OWL), a semantic technology standard for knowledge representation. Security in service access is ensured through multi-factor authentication method. Authenticated access is further restricted through authorization making use of user's defined roles and relationships. This paper demonstrates an implementation of secure service access by means of authentication and authorization through personal and corporate or social identities.

The paper starts with the definitions of identity and its management emphasizing the motivation of terming roles and relations as identity of users (section 2). Section 3 introduces semantic technologies and discusses the motivation behind the use of them. The paper then illustrates

[1]Telecom & IT research reports by RNCOS, *European Mobile Market Scenario to 2012*, `http://www.rncos.com/Report/IM101.htm` [retrieved on Jan. 17, 2009]

the generic architecture of the proposed identity handling mechanism in section 4. Section 5 addresses the security requirements and methods of the proposed identity mechanism bringing the detail authentication and authorization aspects. Section 6 presents the concept of service interaction using the distributed identity mechanism and shows the prototypical implementation of the presented concept. The paper will review some of the related works and then provide critical analysis on different aspects of the proposed distributed identity mechanism in section 7 and 8. The paper concludes with a summary of the paper and comments on future research.

2. Identity

In this section, we look for the definitions of identity from different angles and explain how these definitions motivate us to extend the social aspects of identity with a goal to interact services securely.

2.1 Definition of Identity

In social sciences, Identity is broadly used to describe an individual's comprehension of him or herself as a discrete, separate entity[2]. Analyzing the current usage of identity in ordinary language and social science discourse, it can be summarized that identity is currently used mainly in two linked senses, 'social' and 'personal' [10]. In the former, a person is distinguished by rules deciding membership and characteristic features or attributes. In the second sense, identity is distinguishing characteristics that a person takes a special pride in. 'How people relate to others' is termed as identity by [15]. It 'refers to the ways in which individuals and collectivities are distinguished in their social relations with other individuals and collectivities' [19]. According to Dick Hardt, CEO of Sxip Identity, identity is also what i prefer, what my interests are, what my roles are in real life [14].

In this paper, we take into account both the 'personal' and 'social' sense of identity. 'Personal' sense is realized through possessing or knowing some identifying characteristics and the later is established through roles and relationships of an individual.

2.2 Role as Identity

Central to the identity theory developed by Stryker [32], McCall and Simmons [24], and Turner [34] is the concept of role identities. The Theory links self attitudes, or identities, to the role relationships and role-related behavior of individuals. The theorists argue that the self consists of a collection of identities, each of which is based on occupying a particular role. Stryker said 'the number of identities is limited only by the number of structured role relation ships one is involved in' [32].

2.3 Relationship as Identity

In the Social Identity Theory [33], beyond the 'personal self' a person has several selves that correspond to widening circles of group membership. Apart from 'personal self', an individual has multiple social identities. Social identity is the individual's self-concept derived from perceived membership of social groups [16]. The group membership creates positive self-esteem by positively differentiating their ingroup from a comparison outgroup on some valued dimension. Because of these, people's sense of who they are is defined in terms of 'we' rather than 'I'. Thus the social identity differs from the notion of personal identity which refers to self-knowledge that derives from the individual's unique attributes.

2.4 Paper-based Identity

It is the traditional form of identity. People are carrying a good number of paper-based identities, for example, passport/personal ID, credit cards, bank cards, student card, office ID, driving license etc. with them. Nowadays, people increasingly use smart cards with electronic chip for service access and payment. It enhances the security and allows storage of user details on the card. These are normally used at designated service points that can recognize specific smart cards. The possession factor of such identities are coupled with a knowledge factor like PIN codes, which authenticate the true owner and serve as additional security requirements (this phenomena will be discussed more detailed in section 5). However, with the increasing digitization of identity transaction, many of the paper-based identities are gradually replaced or supplemented by digital identities.

2.5 Digital Identity

Digital identity is the digital representation of a set of claims made by one digital subject about itself or another digital subject. A digital subject can be human or non-human. Instead of set of claims made by parties, digital identity can also be defined as a collection of information that relates to an individual, that is created and managed as a single unit in a network, and that is stored in electronic form[3].

[2]Identity(social science) http://www.answers.com/topic/identity-social-science [retrieved on Jan. 18, 2009]

[3]Definition of digital identity, http://idcorner.org/2005/03/07/on-the-definition-of-digital-identity/ [retrieved on Jan. 18, 2009]

2.6 Identity Management

In information systems, identity management is a broad administrative area that deals with the management of identity life cycle of entities starting from establishing identities and ending with repealing those identities, when required. This is the pure identity paradigm that does not consider access or entitlements. Within the life cycle, identities are described through various attributes. Identity management involves user access paradigm which considers the management of identity associated data required to access a system. User may know these data beforehand or a secure physical device may contain these. Here, entities are identified by presenting these identity associated data. The access to resources within the system can be controlled by associating user roles, rights and restrictions, presence with the established identity. Thus system can deliver personalized services. This is service paradigm perspective of identity management. Therefore, in addition to identity and access manager, identity management solutions[4] [5] also encompass role manager.

In this paper, we are concerned with user access and service paradigm identity management. That is why, we also demonstrated how the proposed distributed identities can facilitate service interaction.

3 Introduction to Semantic Technology

We used semantic technologies to represent part of user's corporate and social identities, and to realize access authorization decisions (detail in section 5). This section introduces the technologies and the motivations of using them in this work.

Semantic Web [4] provides various technologies to capture the knowledge about a domain of interest in the form of concepts and their relationships at different levels of abstraction. It supports the reasoning about both the structures and the properties of the elements that constitute the system. Ontologies [11] are the cornerstone technology of Semantic Web. Among the different ontology languages, the OWL [31] is chosen because it facilitates greater machine interpretability of the Web content than that is supported by XML, RDF, and RDFS by providing additional vocabularies along with formal semantics. RDF/XML syntax is the basis of serialization in OWL ontology. There are three species of OWL: OWL Lite, OWL DL and OWL Full and these are designed to be layered according to their increasing expressiveness.

[4]Oracle Identity Management, `http://www.oracle.com/products/middleware/identity-management/identity-management.html` [retrieved on Jan. 18, 2009].

[5]Sun Identity Management, `http://www.sun.com/software/products/identity/offerings.jsp` [retrieved on Jan. 18, 2009].

Apart from the representation of domain knowledge, the architecture requires more expressivity to deduce decidable conclusions which in fact provide the authorization decisions during controlling access to a system. To enhance the expressivity of the ontology, we decided to use OWL DL which is based on the Description Logics (DL) and amenable to automated reasoning[6]. Though OWL DL lacks in expressivity power compared with OWL Full, it maintains decidability[7] and computational efficiency. The computational efficiency is important since the scheme has to handle many relations.

As the expressivity provided by the OWL is limited by tree like structures [25], the implicit relations representing the restricted access scenarios cannot be inferred from the indirect relations between the entities. These require rule support and interworking with ontologies. One suitable rule language is the Semantic Web Rule Language (SWRL) [17]. Along with SWRL, we also use Semantic Query-Enhanced Web Rule Language (SQWRL[8]) to further enhance the expressivity of OWL, specifically to derive the access authorization decisions based on defined knowledge (ontologies).

4 Generic Architecture of the Identity Handling Mechanism

This chapter introduces the generic architecture of the identity handling mechanism and illustrates each of its components.

4.1 Roles in Life

Every human being plays numerous roles in life to live. As a student, we are attending an educational institute; as a researcher or engineer, we are working in a company; as a consumer, we are buying things with cash or credits; we are maintaining social relationships with family, relatives, neighbors and colleagues. While exercising these roles in life, we are interacting with many service providers to receive different types of services. For example, as a student one has access to various services of the institute. Analyzing these scenarios, it can be said that every human being plays roles basically in three different areas, personal, professional and social areas. Therefore in reality, leading everyday life is nothing but playing some personal roles, professional roles and social roles in general.

[6]Reasoning is the process of deducing implicit or indirect relations from the explicit knowledge.

[7]Logics are decidable if computations/algorithms based on the logic will terminate in a finite time.

[8]Semantic Query-Enhanced Web Rule Language (SQWRL), `http://protege.cim3.net/cgi-bin/wiki.pl?SQWRL` [retrieved on Jan. 18, 2009]

In this article, we are proposing a concept of 'My digital identity' which contains 'My personal identity (PID)', 'My corporate identity (CID)' and 'My social identity (SID)' that would represent ourselves and our relevant real life roles to the digital world. 'My personal identity' can be used to identify ourselves in our personal and commercial interactions. Similarly, 'My corporate identity' and 'My social identity' can be used in our professional and interpersonal interactions respectively.

4.2 Personal, Corporate and Social Identities

Each of these three identities will have several identifiers. Each identifier will be used to access several relevant services and a number of attributes will characterize an identifier (see figure 1). Attributes are those set of characteristics of an identifier that are required by the service providers during service interactions. For example, passport can be one of the identifiers and name, date of birth, date of issue, date of expiry, the country that issued the passport, passport number etc. can be its attributes. The passport

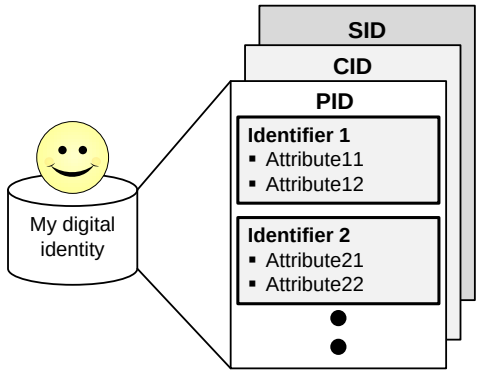

Figure 1. Generic architecture of 'My digital identity'.

that is in fact the most important personal identity issued by the government and used to deal with many government or non-government services. Similarly, another identifier will be used to get access to financial services, like, buying something through credit cards. Attributes of such identifiers are name of the person who holds the credit card (may be optional), number of the card, pin code, date of expiry etc. My PID might have some more identifiers to access our home premises, home network or VPN etc. In the same way, My CID and My SID will have several such identifiers and attributes. My CID might hold the identifiers to access our office premises, office LAN/VPN etc. According to Dick Hardt, individual's interests, fondness, preferences or tastes are also part of his/her identity [14]. In the proposed identity model, these features will also be dealt with by My CID and SID through roles and relations. It may also include identifiers for accessing my email, messenger, IP telephony etc. Each identifier will contain only the required identifying information that a service provider needs to know. 'My digital identity' thus, ensures the minimum disclosure of identifying information.

4.3 Representation of Relationship

Following the research in social science, we proposed the notion of social identity, which in this paper means individual's relationship to a group or with other individuals. Social relation can refer to a multitude of social interactions, regulated by social norms, between two or more people, with each having a social position and performing a social role. We consider the fact that, in the social context we sometime like to be identified as 'member of Cycling Group' or 'Friend of X' etc.

In our research, we represented these social identities using ontologies and we used OWL to design these ontologies. Later (in section 5.3), it is explained how these identities are exploited to authorize a person to see and access group's resources.

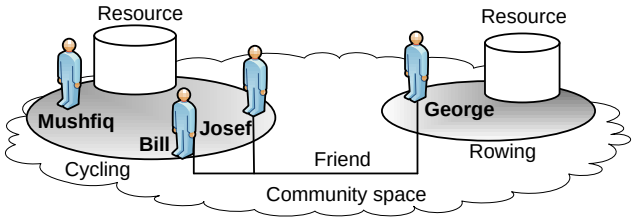

Figure 2. A sample community structure.

Suppose, there exists a community space in the network where there are two communities: Cycling and Rowing, each containing community and public resources. Bill, Josef and Mushfiq are members of Cycling community, while George is a member of Rowing community. Bill, George and Josef are friends to each other. Figure 2 illustrates this sample community structure. The relationship to the community (membership) and the relationship among individuals are exploited to provide access authorization to the right resources. A virtual social network may contain such architecture to ensure security and privacy of community itself and its members. Figure 3 shows the sample codes in RDF/XML (OWL syntax) representing a community environment containing members, some of whom are friends of each other, while some are not.

```
-----
-----
<Community rdf:ID="Cycling">
<hasMember rdf:resource="http://www.owl-ontologies.com/OntologyBill4.owl#Bill"/>
<hasMember rdf:resource="#Mushfiq"/>
<hasMember rdf:resource="#Josef"/>
<hasCommunityResource rdf:resource="http://www.owl-ontologies.com/
OntologyBill4.owl#CyclingPartyVideo"/>
<hasPublicResource rdf:resource="http://www.owl-ontologies.com/
OntologyBill4.owl#HowToCycleVideo"/>
</Community>
<Community rdf:ID="Rowing">
<hasMember rdf:resource="#George"/> </Community>
-----
-----
<owl:Class rdf:ID="Member"/>
<Member rdf:ID="Bill">
<belongTo rdf:resource="#Cycling"/>
<hasFriend rdf:resource="#George"/>
<hasFriend rdf:resource="#Josef"/>
<hasPrivateResource rdf:resource="http://www.owl-ontologies.com/
OntologyBill4.owl#PrivatePartyVideo"/>
</Member>
<Member rdf:ID="Josef"> <belongTo rdf:resource="#Cycling"/>
</Member>
<Member rdf:ID="Mushfiq">
<belongTo rdf:resource="#Cycling"/> </Member>
<Member rdf:ID="George"> <belongTo rdf:resource="#Rowing"/>
</Member>
-----
-----
```

Figure 3. RDF/XML code sample representing a community environment.

4.4 Representation of Role

Individuals gain a social identity and group identity by their affiliation. Individuals play numerous roles in the institutions they are associated with. We distinguish professional institutions from the other social institutions, because the former demands the higher security requirements in participation than the later. Therefore, in this paper we mostly focused on roles an individual plays in professional organization. In this regard we are going to illustrate a specific scenario. Nowadays people in business organizations increasingly work in project oriented environments. The project members come from different departments. The role of each department constitutes at least a supervisor and subordinate employees. Similarly, each project contains a project leader and members. From the sense of identity, we are accustomed to identity ourselves as 'supervisor of department X' or 'project member of project Y', especially in social context. These distinctions of roles play a crucial role in controlling the access to work unit's resources. For this purpose, we also represented this specific scenario of roles using OWL.

Suppose, an organization (a company) consists of two departments: Dept. A and B, each containing some resources. Hans Christian is the supervisor of Dept. B and Josef Noll plays the similar role in Dept. A. Erik Swansson and George Kalman are the employees of Dept. B and A respectively. Figure 4 shows such a sample organizational

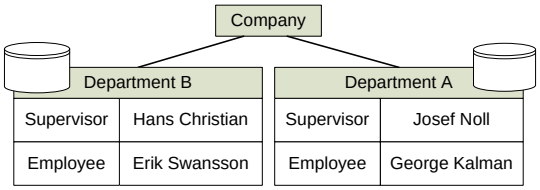

Figure 4. A sample organizational structure.

```
-----
-----
<Department rdf:ID="DepartmentA">
<hasResource rdf:resource="#DeliverableDeptA"/>
<hasResource rdf:resource="#DocDeptA"/>
<hasResource rdf:resource="#AdminResDeptA"/> </Department>
<Department rdf:ID="DepartmentB">
<hasResource rdf:resource="#DeliverableDeptB"/>
<hasResource rdf:resource="#DocDeptB"/>
<hasResource rdf:resource="#AdminResDeptB"/> </Department>
-----
<EmployeeID rdf:ID="Erik_Swansson">
<hasRole rdf:resource="#DeptB_Employee"/> </EmployeeID>
<EmployeeID rdf:ID="George_Kalman">
<hasRole rdf:resource="#DeptA_Employee"/> </EmployeeID>
<EmployeeID rdf:ID="Hans_Christian">
<hasRole rdf:resource="#Supervisor_Hans"/> </EmployeeID>
<EmployeeID rdf:ID="Josef_Noll">
<hasRole rdf:resource="#Supervisor_Josef"/> </EmployeeID>
<Supervisor rdf:ID="Supervisor_Hans">
<rolePlaysIn rdf:resource="#DepartmentB"/> </Supervisor>
<Supervisor rdf:ID="Supervisor_Josef">
<rolePlaysIn rdf:resource="#DepartmentA"/> </Supervisor>
<Dept_Employee rdf:ID="DeptA_Employee">
<rolePlaysIn rdf:resource="#DepartmentA"/> </Supervisor>
<Dept_Employee rdf:ID="DeptB_Employee">
<rolePlaysIn rdf:resource="#DepartmentB"/> </Supervisor>
-----
-----
```

Figure 5. RDF/XML code sample representing an organization.

structure. We will see later (in section 5.3) that depending on roles and relationships to the work units, each individual is authorized to access the right resources. The sample codes in RDF/XML are shown in figure 5.

4.5 Distributed Identity Mechanism

The paper introduces a notion of distributed identity and this section explains the mechanism in detail. With the identity services subscription, Identity Provider (IDP) issues a certificate to the user and allocates a secure identity space in the network. User identity data and attributes are distributed and stored into two places. A part of the user identities that contain very sensitive user information like, PID (e.g., creditcard identifier, home admittance key) will be stored (permanently or temporarily) in the SIM card of mobile phone. This is the primary part of the identities which is used to access the remaining of identities. Therefore, access to these requires strict authentication. The other part of user identities which need medium/low authentication requirements,

Table 1. The PID, CID and SID, their realization, storage location and security requirements.

Identity	Examples	Realization	Location	Security requirements
PID	PID (Credit card)	Certificate + key (public + private)	SIM	High
	PID (Home admittance)	Fixed binary key	SIM	High
CID	CID (Office admittance)	Fixed binary key	SIM	High
	CID (Office admittance)	Temp. binary key	Network	Medium
	CID profile (Role)	foaf/OWL (RDF+XML)	Network	Medium
SID	SID profile (Relation)	foaf/OWL (RDF+XML)	Network	Medium/Low

for example social identities and preferences (SID), will be stored into the secure identity space in the network. Table 1 gives several examples of PIDs, CIDs and SIDs, their possible realizations and where these identities will be located or stored. Considering the various levels of security, the corresponding security requirement of each identity is also mentioned.

During the subscription, an operator can load the SIM card with a private key for the user. PID credentials are realized through certificates and keys provided from the Banks. These can also be stored in the SIM card. The trusted third party (whoever it is) can mediate the whole process. There are few possibilities of realizing PID for home admittance. Admittance keys can directly be stored in binary format in the SIM card or a hash can be generated from the stored private key and hash algorithm. The keys or a hash can later be transferred to other devices using NFC technology. CID and SID profiles and preferences are realized using either FOAF (friend of a friend) or Web Ontology Language (OWL) and stored these foaf/owl files in the network. We think Semantic Web Technology (foaf/OWL) can provide solutions to access control and privacy in corporate and social environment by defining users' roles, relations and access and privacy policies. We have already represented such provisions in OWL implementing identity handling, access control and privacy support in corporate and social community areas in a separate work [8]. Detail description of the work is beyond the scope of this paper. However, we introduce the motivation of using Semantic Technologies for the purpose of security and privacy assurance in section 3

4.6 The Role of Identity Providers

The role of an identity provider is very crucial in identity provisioning. Similar to the subscription of voice and data services, access to identity services subjects to explicit agreement between users and identity providers. An IDP is maintaining strong trust relationships among the subscribers, service providers and the other IDPs. Identity providers may come from users social, corporate or personal domain. Security requirements of identity provisioning from these domains depend on the relevant service access security demands. State/government is the traditional and most accepted identity provider in national and international level providing citizen ID. With strong regulations in place (by state), banks and mobile operators can also act as an IDP. Having a state or citizen ID is obligatory to establish access to some of these services. Several service access (e.g., access to Banks or Creditcards) requires high security environments and therefore the roles of these IDPs are strictly regulated.

4.7 SIM as Identity Storage Element

The SIM card is considered as secure identity storage place because it can be revoked, there are possibilities of further security enhancements in it and user now-a-days can rarely be found without a mobile phone. High capacity SIM cards are available in the industry with increased memory size, additional cryptographic and high speed communication (SIM-handset, SIM-network) capabilities [35]. Handling identities from the SIM gives the user control over the usage of his identities. It is expected that IDPs do not own or control SIM card rather act as facilitators to manage identities. To manage multiple credentials, IDPs can load additional IDs confidentially to either a SIM card (with over-the-air provisioning) or at network identity space with user's consent. In case of loosing the SIM card, a new one can be ordered and the identities previously stored in the card can be reloaded.

With the identity subscription certificate user can identify himself to access the network identity repository that contains identities for example SIDs. These identities will be used to access services that need medium or low level of security requirements. The SIM card holds only the most sensitive user identities. As the network is vulnerable to many security threats, only information of less sensitive character are stored in the network.

5 Security Mechanism

This section discusses the security mechanism introducing the levels of security and explaining the authentication and authorization methods in detail.

5.1 Levels of Security

Ensuring secure service access using proposed identity mechanism is a challenging issue, considering the fact that we are going to store part of the identity in the network that is vulnerable to electronic attack. It has been proposed in this paper that the mobile phone will act as the primary device to access 'My digital identity' in the network. In addition to this, a part of the identity that requires the highest security will be stored in mobile phone SIM card. Here, it is assumed that the user has the provision for 'always-on' functionality in his mobile phone.

Access control is a general way to ensure security in accessing services and resources in the Web. It mainly includes Authentication and Authorization. These two meet two different security requirements. The former verifies user's identity and the authorization assures users rights in a system. Moreover, multi-factor authentication enhances the security of authentication mechanism.

Different levels of authentication mechanisms need to be maintained depending on service access security requirements. From user point of view, a securely maintained communication channel is required to exchange very sensitive user information with the service provider. There are services that require only little information about the user. Highly secured infrastructure is not a necessity for them. Besides, building or maintaining very secure channel requires good investment as well. Therefore, different levels of security should be employed for different types of services. Analyzing all these aspects, [27] introduced three levels of security: Nice to know, need to know, have to know according the increasing security requirements (see figure 6).

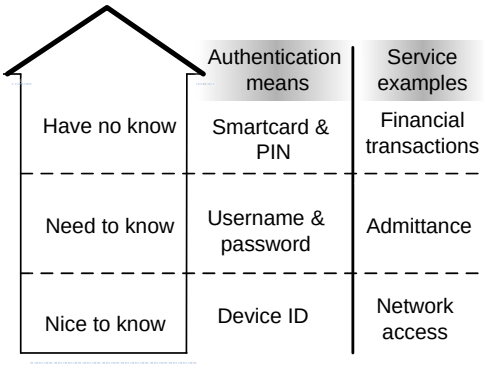

Figure 6. Levels of security based on security requirements of services.

5.2 Authentication

Authentication is the process of identifying an individual. It gives individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about access rights of individuals.

5.2.1 Multi-factor Authentication

An authentication factor is the information or the process used to authenticate or verify the identity of an entity requesting access to a system under security constraints. There are generally three types of authentication factors (listed from weakest to strongest): something a user knows (e.g., password), something a user has (e.g., security token), and something a user is or does (e.g., biometrics). The process of combining multiple authentication factors is called multi-factor authentication. Single factor authentication can be compromised quite easily. Hence, multiple factors can make the authentication stronger.

In the proposed system, we also include multi-factor authentication mechanism. Through a nice to know authentication method, user can access 'My digital identity' and, through a need to know authentication mean, user can access most other services, such as, accessing messenger (msn or yahoo), my address book, voip services, e-mail account; accessing home or office premises etc. Nice to know services are network access, where knowledge about usage is only required. Access to a very personal device like, SIM of a mobile phone (it contains unique identifier), can provide nice to know authentication to the network. Need to know services have higher security requirements. In addition to the device identifier, these require passwords or PIN. If the mobile phone usage is PIN protected, need to know authentication can be avoided. Highest security requirements are needed for have to know services. Users have to be authenticated through a have to know authentication mechanism to use the identifiers that are necessary to access financial services such as, banking, online shopping etc. Here, we are proposing to deploy the have to know authentication mechanism in SIM card through Public Key Infrastructure (PKI). Thus SIM card will be a part of 'My digital identity'. This will significantly minimize the possibility of disclosure of identities for financial services, in case there are electronic attacks on network contents of 'My digital identity'.

5.2.2 Extended SIM Card Authentication

Currently, the SIM card provides the nice to know access to network. We propose that the SIM card authentication will also be enough to enter the part of 'My digital identity' located in the network. The higher security requirements that

need to know services may require might also be satisfied through SIM card authentication [27].

As proposed, the have to know authentication mechanisms will be realized in SIM card. Hence, we are introducing an extended SIM card (ESIM) is a customized variant of USIM (Universal Subscriber Identity Module) and it has the capability to hold multiple credentials. One will be responsible to provide the nice to know and need to know authentications and another one will store the have to know authentication mechanisms. ESIM will also be a part of 'My digital identity' which the users will always carry.

The have to know authentication mechanism in SIM card can be realized by implementing PKI. PKI enables users to secure a public network (e.g., Internet) through using public and private cryptographic key pair that is obtained and shared through trusted authority (Certificate Authority) [13]. In mobile networks, there exists a formal relationship between users/subscribers on one hand and the network operator of the other. Therefore, network operator can naturally play the role of Certification Authority (CA). The users private key as well as the root CA public key can be distributed in a secure way in the form of SIM card. The formal relationship, which the operators already have through roaming agreement, could be extended to cross-certification of each other public keys. Mobile network operators therefore are in a very strong position to establish themselves as CAs, and the mobile device naturally lends itself to become a secure storage medium for these cryptographic keys [20].

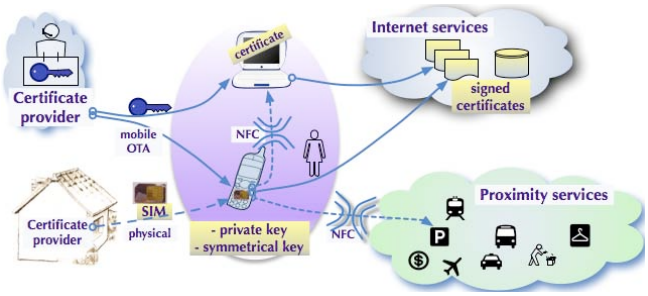

Figure 7. SIM based certificate and key handling.

PKI enables the parties in a dialogue to establish confidentiality, message integrity and user authentications without having to exchange any secret information in advance. Figure 7 illustrates SIM based certificate and key handling provisions. Certificates can be provided to the mobile phone either physically or through mobile over-the-air (OTA)[9] provisioning. It is possible to sign the certificate/transactions using stored private key from the mobile phone or PC. These signed certificate/transactions will provide authentication, integrity and non-repudiation services during service interactions.

[9]Over-the-air (OTA) is a standard for the transmission and reception of application-related information in a wireless communications system.

5.2.3 Acceptability of Mobile Phone as Identifier

Nowadays mobility of people increases due to dynamic life style and working nature. The mobile phone has become a foremost electronic device not only for communication but also for managing different other activities, such as, banking, collecting information from web, checking emails etc. Mobile phone penetration is expected to reach 100% in most of the developed countries. So, the basic infrastructure to use the mobile phone as identifier is already in place. Currently, different types of access systems can be found in wireless networks. Services are expected to be interoperable in different wireless communication systems. A SIM is a temper resistant device in a wireless system holding subscriber identity and authentication information. The SIM card in the mobile phone has the capability to provide all levels of authentication, and support mechanisms for revocation of credentials stored in the SIM card [26]. It is only active if authenticated by the network operator. If it gets stolen, the operator can disable the card. SIM card opens for authentication and encryption in every wireless network (Bluetooth, WLAN, WiMAX) in addition to GSM and UMTS [26]. So, SIM card enables authentication mechanism to interact different services will certainly give a technological edge to the development of future wireless technologies and services. By storing a part of the identity in the network, we are reducing the volume of data transfer from mobile phone to network. In consequence, the additional data transfer due to the use of such system will leave a very little effect on the capacity of air interface. Therefore, the acceptabilirty of mobile phone as identifier is expected to be very high.

5.3 Authorization

When a user is authenticated, information system has to make sure that he accesses only what he is allowed to. Access authorization determines a) what an user can do in a system (access to contents/services) and b) with which privileges? (e.g., read and/or write over the contents).

5.3.1 Authorization Based on Relationships

In this section, we refer to the representation of identity (relationship) to discuss the authorization based on relationships. Access authorization decisions are derived based on the relationship among the individuals, and between the individuals and the community they belong to. Bill, Josef and Mushfiq belong to the Cycling community; George belongs

to the Rowing community; Bill has two friends: George and Josef, and he also possesses a private resource: Private Party Video. Cycling community has community and public resource. From this scenario, we are expecting the following access situations:

- Cycling community members (Bill, Josef and Mushfiq) can access community resource: Cycling Party Video with full access privilege (streaming and download the full length).
- Josef is expected to get full access to Bill's private resource: Private Party Video, as he is not only a friend of Bill, but they also belong to the same community.
- George gets limited access (preview only) to Cycling Party Video as he is not a member of Cycling community.
- George is allowed to see the Private Party Video of Bill with limited access privilege though he is a friend of Bill, as they are not in the same community.
- Mushfiq can see the Private Party Video of Bill with limited access privilege as he is not a friend of Bill, though they belong to the same community.

These access situations are realized through a set of access authorization policies and they are designed through rules exploiting SWRL. Figure 8 illustrates these policy

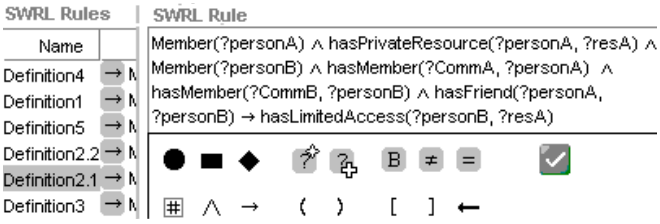

Figure 8. Access policies are designed through rule using SWRL.

sets and a snapshot of one of the rules. The rules executed using Jess rule engine to derive the access authorization decisions. Figure 9 shows the authorization decisions which follow the defined access situations. The access privileges are not shown in the figure but these are working from the back end.

5.3.2 Authorization Based on Roles

In section 4.4, we have represented an organizational environment containing different work units, employees, their roles and relationships with relevant work units. Table 2 shows the detail organization structure containing roles and

Person	Access to Resource
Bill	CyclingPartyVideo1
Josef	CyclingPartyVideo1
Mushfiq	CyclingPartyVideo1
Josef	PrivatePartyVideo1
George	CyclingPartyVideo1
George	PrivatePartyVideo1
Mushfiq	PrivatePartyVideo1

Figure 9. Access authorization decisions derived executing SWRL rule shown in figure 8.

Table 2. The detailed organizational structure with roles and privileges of each employee.

Employee Name	Work Unit	Role	Privilege
Josef Noll	Dept. A	Supervisor	Administrator Final Approval Read & Write
George Kalman	Dept. A	Employee	Read & Write
Hans Christian	Dept. B	Supervisor	Administrator Final Approval Read & Write
Erik Swansson	Dept. B	Employee	Read & Write

privileges of each employee. In this section, we will see how an employee can access to the right work unit's resources based on his defined roles and relationships. In this case, the expected access situation are,

- Hans Christian and Josef Noll work as supervisor in department A and B. They hold privileges: Administrator, Read & Write and Final Approval. Therefore, they are expected to administer relevant department's administrative resources, give final approval to deliverables, and read and write ordinary documents.
- Erik Swansson and George Kalman work as employee of the department. They possess only Read & Write privilege. Hence, they should only read and write relevant department's ordinary documents.

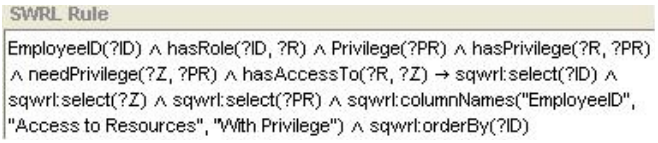

Figure 10. Rules (SWRL) along with queries (SQWRL).

A common access policy is designed according to these situations through rule using SWRL and figure 10 shows

EmployeeID	Access to Resources	With Privilege
Erik_Swansson	DocDeptB	ReadWrite
George_Kalman	DocDeptA	ReadWrite
Hans_Christian	AdminResDeptB	Admin
Hans_Christian	DocDeptB	ReadWrite
Hans_Christian	DocDeptB	ReadWrite
Hans_Christian	DeliverableDeptB	FinalApproval
Josef_Noll	AdminResDeptA	Admin
Josef_Noll	DocDeptA	ReadWrite
Josef_Noll	DocDeptA	ReadWrite
Josef_Noll	DeliverableDeptA	FinalApproval

Figure 11. Access authorization decisions derived executing rule and queries of figure 10.

the rule. Jess rule engine executed this rule and derived the access authorization decisions. The decisions are displayed in figure 11 and employees are found to get desired access to the right resources.

6 Service Interaction

This section presents a service interaction concept and demonstrates a practical implementation of a sample service interaction involving proposed authentication and authorization mechanism.

6.1 Service Interaction through Distributed Identity

A concept of service interaction using distributed identity is introduced here. Figure 12 shows graphical representation of the concept. My digital identity consists of PID,

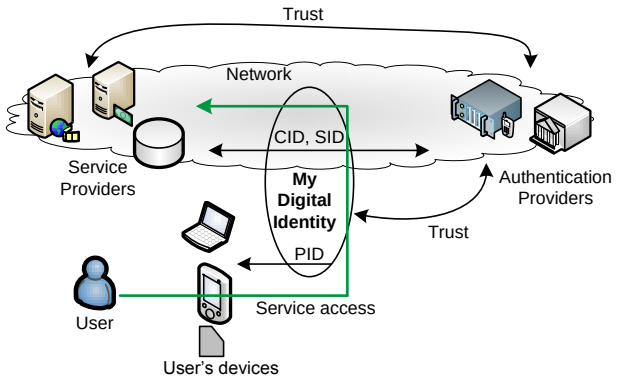

Figure 12. Concept of service interaction through distributed identity.

CID and SID. User personal device (e.g., SIM of mobile phone) stores PID, and CID and SID are stored mainly in the network. The later mostly are the roles and relationships of the users. Authentication providers (e.g., Bank, Government, Mobile Operators) provides the PIDs, and the roles and relationships are defined either by the user himself or by the proper authorities. The final goal is to interact the services offered by their providers through my digital identity. In this regard, users need to be authenticated and authorized. Authentication is done through PIDs and Authorization is done through role and relationships which are part of CID and SID. To facilitate the service interaction, the service providers and authentication providers should trust each other. In addition, authentication providers and users should also maintain strong trust relations. However, trust mechanism is beyond the scope of this paper. The next section presents a prototypical implementation of service access involving authentication and authorization mechanism. Authentication is done with stored binary key and authorization is realized through roles and relationships.

6.2 Prototypical Implementation of Service Access

The demonstration includes a mobile based key distribution and thereby authentication to a service by the key. It was built based on an earlier implementation of NFC-based key distribution and admittance [27]. The key generation and distribution was modified to support online access to contents of a service provider (SP). The authentication provider generates key upon request and transmit to the user through mobile phone system. The key is stored in integrated smartcard and transmitted on demand to the mobile terminal. The terminal can itself access services based on that key or, as demonstrated, can be used to perform user identification where higher security is required. In our service example, the key is transmitted over the NFC interface towards SP.

User wants to access contents remotely from a service provider using the PC. Figure 13 illustrates the steps of service access demonstration. In step 1, the access request is sent to the SP. Triggered by the request, in step 2, access control system of the provider sends a message to the authentication provider. This entity transmits access information and an access key to the mobile phone of user. We assume that Service and authentication provider belong to a common trust system and user's mobile phone number is sent to SP during service access request. The user authentication provider creates an information message (3) and a binary key (4), which is transmitted to the user's phone (here Nokia 3320) and stored in the SmartMX card of its NFC unit. The key can be transmitted over the NFC interface to NFC-enabled devices. In case, services are accessed from the PC, the key is transmitted to the PC using near field

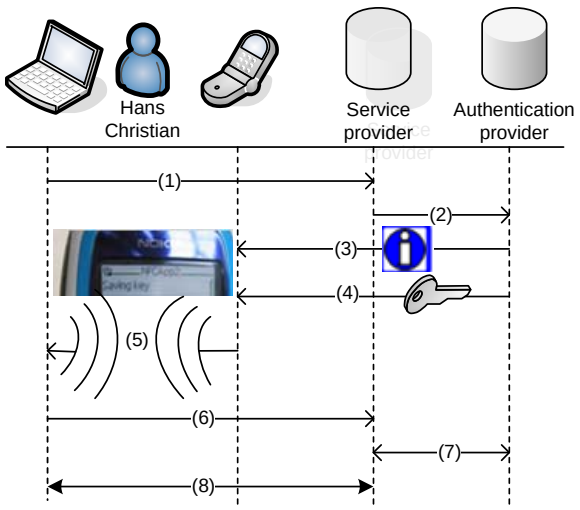

Figure 13. Prototype of online content access.

communication (5). User then presents the key to the SP (6), it then validates the key (7), and finally user gets the authenticated access (8). If services are accessed from the mobile phone, the phone number can even validate the key, provided SP has previous knowledge of key holder's phone number. Service providers also need the capability to identify the phone number from the initial service request message (1). Our implementation used Telenor's mobile network through PATS Innovation lab[10].

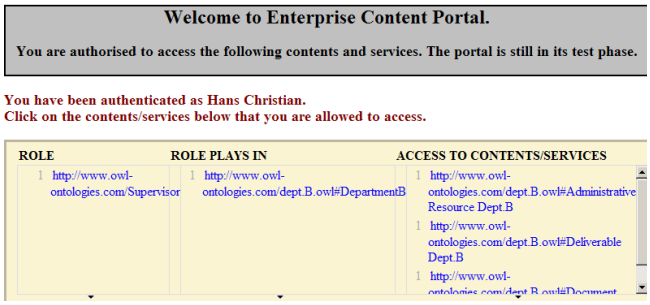

Figure 14. Prototype of access authorization to enterprise contents.

The objective is to access contents from a system of an enterprise with appropriate privileges when, each of the users has predefined roles within the organization. Hans Christian has just been authenticated by presenting a key to an enterprise content/service provider. Figure 14 illustrates a front end of the provider's content/service management system. It shows the contents, Hans Christian is authorized to access. We have seen from the discussion before that Hans is a supervisor of department B and he is permitted to access administrative resources, deliverables and documents of department B with administrator, read & write and final approval privilege. Privileges are working from the back end of the system.

[10]PATS (Program for Advanced Telecom Services), `http://www.pats.no` [retrieved on Jan. 18, 2009]

7 Related Work

This section brings in literatures and research related to secure access specifically in the area of access authorization. In this paper, we introduced user's corporate and social identities through roles and relationships. Access authorization is realized using the formal description of these roles and relationships. We are going to review some of the relevant works in this section.

Role Based Access Control (RBAC) [29] is an increasingly popular and efficient solution where users access permissions are associated with the roles, and users are made members of appropriate roles. We consider the concept of RBAC as a part of our access authorization mechanism. Besides incorporating the notion of roles, the proposed architecture includes the attribute which states 'where (department or project) one plays the roles'. Therefore, a simple notion of Attribute Based Access Control (ABAC) [36] has also been integrated in this architecture. This further restricts the relevant access authorization (toward the specific work unit) decisions. Role as a basis for authorization enables the use of constraints to support Separation of Duty (SoD). SoD is widely considered to be a fundamental precept in computer security [9],[28]. In brief, the principle states that if a sensitive task is composed of two steps, different user should do each step. We can interpret this definition in the context of the organizational environment illustrated in section 5.3. To deliver a final audit report, employee of audit department should get access to the report only to read and write specific entries but supervisor of the department has the authority to give final approval to it. In this paper, we ensure this to happen though through simple static role assignment.

In social community environment, we have chosen the relationship of an individual with the community (*member*) or with the fellow individuals (*family or friend*) as a basis to authorize access to private or community resources. Instead of relations, a concept of trust or reputation can also facilitate the access authorization [7]. In this regard, [12] introduced a distributed trust management approach to provide access to community resources. From the context of this paper, trust cannot be considered as identity traits of a person and therefore, this should not be used as the only mean to authorize access to private resources. However, the trust coupled with relationship can strengthen the privacy in

virtual community networks.

We represented the access authorization policies using OWL and SWRL. XACML (eXtensible Access Control Markup Language) is a popular access control policy language [23]. In [22], authors suggested expressing the access control policies based on OWL and SWRL citing the lack of formal semantics in XACML. KAoS [5] and Rei [21] are the two noticeable works in this regard. Policy specification language in Rei is based on OWL Lite which is less expressive compared with OWL DL. In [18], a Semantic Based Access Control Model was presented which considered semantic relations among different entities in decision making process. Therefore, use of formal representation of roles and relationships for access authorization is gaining momentum to secure a social or organization community space.

8 Discussion

This section introduces several other critical features of the proposed identity mechanism. In the 'Laws of Identity', Kim Cameron states that any sustainable and universally adopted identity architecture must only reveal the least identifying information possible with the users consent [6]. In the proposed identity mechanism, user controls how much identifying information it would reveal to the service providers by controlling the access to the primary storage of the identities (SIM card). As the services are accessed only through relevant identifiers of the PID, CID or SID, minimal disclosure of only necessary identifying information with users consent is ensured.

Sxip [2] and Windows CardSpace [3] are the two identity solutions developed by Sxip identity and Microsoft Corporation. In Sxip, membersites are typical websites that consume identity data by sending Sxip requests for user data to homesites, also websites that store user identity data. Homesites authenticate and identify users. It uses two-factor authentication solution to access services, like, online banking that requires strong authentication mechanism. Sxip 2.0 can use a third party credentials which is an interesting way to hide the use of PKI behind a software layer. Windows CardSpace uses a variety of virtual cards, each retrieving security token from the identity providers for authentication and identification to services. For greater security, user protects cards with personal identification number (PIN). To provide further assurance of secure communication, Microsoft together with other partners in industry is expected to create a new level of certificate that might contain more information than a traditional Secure Sockets Layer (SSL) certificate. These two identity solutions provide the movement of identity data over the Internet.

Storing the primary part of the identities in mobile phone provides the major advantage over the other available identity mechanisms. It is available 24 h/7 days a week, as compared to about 4 h average usage of a PC. Thus, it provides the always online functionality with availability. As, SIM card may also provide need to know authentication, some services that require minimum security can be available to the users as soon as they enter the proposed identity repository by mobile phone. Deployment of have to know authentication mechanism in SIM (ESIM) not only enhances the security to access financial services but also increases the acceptability of this identity to users. One of the useful features is portability of identifier from one device to another, especially to the devices that has no direct connectivity to 'My digital identity'. Thus, these identities can be accessed from anywhere and service continuity is possible in heterogeneous wireless environment. In case of losing or theft of SIM, we can use our PC to access 'My digital identity' which is optional and demands modification or enhancement of existing security mechanisms.

The proposed identity mechanism will create values for the users, network operators and service providers. User can use a unique identity mechanism that is simple, easy to use, digital in nature but available anywhere and portable to any device. It has the potential to replace many of the paper-based identities, such as credit card, admittance card etc. Network operators can also earn revenues by providing space for the identity repository and facilitating the additional data transfer that the system requires. As there are trust relationships among the parties involved in transactions here, the integrity and confidentiality of the transactions are ensured. Once 'My digital identity' repositories are known to the service providers, new offers can even be posted directly to these repositories.

In addition to effortless movement of identity over the Internet, the proposed mechanism supports the portability of identity data among the devices. Authentication and identification provided by the SIM card is the principle distinctive feature of it. The federated identity standards provided by the Liberty Alliance project[11] also used mobile phone identifier to access Web services. In this paper, PKI based have to know authentication mechanism has been moved to SIM card to reduce the security vulnerability. The Web-PKI suffers from insecure distribution and storage of cryptographic keys and therefore does not provide a complete chain of trust [20]. By combining the roles of CA, mobile network operators would make it easier to have a complete chain of trust around PKI because there already exists a trust relationship between mobile network operators and their customers. Gemalto, one of the leading digital security providers, is using high capacity SIM card for storing digital certificates or rights [1]. The identity repository can be used instead to store these rights that can be accessed

[11] Liberty Alliance Project, `http://www.projectliberty.org/` [retrieved on Jan. 18, 2009]

through mobile phone. Thus, some overheads during data transfer can be avoided. The mechanism also ensures the portability of rights. There are many identities based on chip cards, like, memory cards and smart cards [30]. There are multiple chip cards, provided by multiple entities and single chip card, shared by few entities. If the proposed identity repository is available in the network which can be accessed anytime and from anywhere through an always online mobile phone, such various identity based chip cards might not be necessary. User needs only one smart card, ESIM card.

9 Conclusion

The paper presented a concept of digital identity, a mechanism of its management, its security infrastructures, and demonstrated a prototypical service interaction implementation. User identities are classified into personal, corporate and social identities. Part of these identities which require the highest security are going to be placed in user's personal device. The Web contains the rest of the identities. We believe the mobile phone's SIM card has the potential to be the secure personal device. User's corporate and social identities are represented through roles and relationships. Secure service access is ensured by means of authentication and authorization mechanism. Personal identifier authenticates user and authorization is achieved through user's roles and relationships. A practical implementation is demonstrated which exploits the proposed authentication and authorization mechanism. In our future work, we will focus on practical implementation of a use case that supports seamless service access in heterogeneous wireless networks using the proposed identity mechanism.

References

[1] Gemalto, a leading digital security provider. `http://www.gemalto.com` *[retrieved on Oct. 11, 2008]*.

[2] The Simple eXtensible Identity Protocol, Sxip. `http://sxip.net/` *[retrieved Oct. 11, 2008]*.

[3] Windows CardSpace. `http://cardspace.netfx3.com/` *[retrieved Oct. 11, 2008]*.

[4] T. Berners-Lee, J. A. Hendler, and O. Lassila. The semantic web. *Scientific American Magazine*, 284(5):34–43, May 2001.

[5] J. M. Bradshaw, S. Dutfield, P. Benoit, and J. D. Woolley. KAoS: Toward an industrial-strength open agent architecture. *In Software Agents, J. M. Bradshaw (ed.), AAAI press*, pages 375–418, 1997.

[6] K. Cameron. The Laws of Identity. `http://www.identityblog.com` *[retrieved Oct. 11, 2008]*, December 2005.

[7] H.-C. Choi, S. R. Kruk, S. Grzonkowski, K. Stankiewicz, B. Davis, and J. G. Breslin. Trust models for community-aware identity management. *In Architecture and Philosophy of the Web Identity, Reference, and the Web. IRW2006/WWW2006 Workshop, Scotland*, May 2006.

[8] M. M. R. Chowdhury, J. Noll, and J. M. Gomez. Enabling access control and privacy through ontology. *In the proceedings of 4th International Conference on Innovations in Information Technology, 2007, Innovations '07, Dubai*, pages 168–172, November 2007.

[9] D. D. Clark and D. R. Wilson. A comparision of commercial and military computer security policies. *In Proceedings of the 1987 IEEE Symposium on Security and Privacy*, pages 184–194, April 1987.

[10] J. D. Fearon. What is identity (as we now use the word)? *Working paper,* `http://www.stanford.edu/~jfearon/papers/iden1v2.pdf` *[retrieved on Oct. 22, 2008]*, 1999.

[11] D. Fensel. *Ontologies: A silver bullet for knowledge management and electronic commerce (2nd ed.)*. Springer-Verlag, Heidelberg, 2003.

[12] T. Finin and A. Joshi. Agents, trust, and information access on the semantic web. *ACM SIGMOD, Special Issue: Special section on semantic web and data management*, 31, 5:30–35, May 2002.

[13] T. O. Group. Public key infrastructure standards. *http://archive.opengroup.org/public/tech/security/pki/index.htm [retrieved on Oct. 11, 2008]*.

[14] D. Hardt. Identity 2.0. *Presented at OSCON 2005, http://www.identity20.com/media/OSCON2005/ [[retrieved on Oct. 08, 2008]]*.

[15] M. Hogg and D. Abrams. *Social Identifications: A Social Psychology of Intergroup Relations and Group Processes*. Routledge, London, 1988.

[16] M. A. Hogg and G. M. Vaughan. *Social Psychology (3rd ed.)*. Prentice Hall, London, 2002.

[17] I. Horrocks, P. F. Patel-Schneider, H. Boley, S. Tabet, B. Grosof, and M. Dean. SWRL: A semantic web rule language combining OWL and RuleML. *W3C Member Submission*, May 2004.

[18] S. Javanmardi, M. Amini, R. Jalili, and Y. Ganjisaffari. SBAC: Semantic Based Access Control. *In the proceedings of the 11th Nordic Workshop on Security IT Systems, Linkoping, Sweden*, pages 157–168, October 2006.

[19] R. Jenkins. *Social Identity*. Routledge, London, 1996.

[20] A. Jsang and G. Sanderud. Security in mobile communications: Challenges and opportunities. *In the proceedings of the Australasian Information Security Workshop, Adelaide, Australia*, February 2003.

[21] L. Kagal. Rei:A Policy Language for the Me-Centric Project. *TechReport, HP Labs*, September 2002.

[22] H. Li, X. Zhang, H. Wu, and Y. Qu. Design and Application of Rule Based Access Control Policies. *In proceedings of the International Semantic Web Conference Workshop on Semantic Web and Policy*, pages 34–41, 2005.

[23] M. Lorch, S. Proctor, R. Lepro, D. Kafura, and S. Shah. First experience using XACL for access control in distributed systems. *In proceedings of ACM Workshop on XML Security, VA, USA*, October 2003.

[24] G. J. McCall and R. Simmons. *Identities and Interactions*. NewYork: Free Press.., 1966.

[25] B. Motik, U. Sattler, and R. Studer. Query answering for OWL-DL with rules. *Proceedings of International Semantic Web Conference*, pages 549–563, 2004.

[26] J. Noll. Services and applications in future wireless networks. *In Telektronikk, Q4/2006*.

[27] J. Noll, J. C. L. Calvet, and K. Myksvoll. Admittance Services through Mobile Phone Short Messages. *Proceedings of the International Multi-Conference on Computing in the Global Information Technology (ICCGI 2006)*, pages 77–82, July 2006.

[28] J. H. Saltzer and M. D. Schroeder. The protection of information in computer systems. *In Proceedings of the IEEE*, 63, 9:1278–1308, September 1975.

[29] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-based access control models. *IEEE Computer*, 29, 2:38–47, February 1996.

[30] S. Sengodan. On secure mobile identity provisioning. *In the proceedings of Wireless World Research Forum Meeting 15, Paris, France*, December 2005.

[31] M. K. Smith, C. Welty, and D. L. McGuinness. OWL Web Ontology Language guide. *W3C Recommendation*, February 2004.

[32] S. Stryker. *Symbolic Interactionism*. Menlo Park, CA: Benjamin/Cummings., 1980.

[33] H. Tajfel and J. Turner. An integrative theory of intergroup conflict. *In William G. Austin, Stephen Worchel (ed.), The Social Psychology of Intergroup Relations. Monterey, CA: Brooks-Cole*, pages 94–109, 1979.

[34] R. H. Turner. The Role and the Person. *American Journal of Sociology*, 84:1–23, 1978.

[35] White Paper. High capacity SIMs. *http://visionmobile.com/whitepapers.html [retrieved on Oct. 11, 2008]*, March 2006.

[36] E. Yuan and J. Tong. Attributed based access control (ABAC) for web services. *In the proceedings of the IEEE International Conference on Web Services (ICWS05), Orlando, Florida*, pages 561–569, 2005.