Access Control and Privacy Enhancement through Role-based Identity Management

MOHAMMAD M.R. CHOWDHURY, JOSEF NOLL

Mohammad M.R. Chowdhury is a PhD student at UniK, Kjeller

Josef Noll holds a professor stipend at University of Oslo/ UniK

Managing user identities for information security and privacy in today's connected systems is a crucial issue. This paper focuses on the access control and privacy problems in a project based business environment to access project resources and to maintain privacy of members. In this regard, a semantic ontology is proposed which formalizes roles of the members, and controls access to project resources by means of formalized privacy policies and rules.

1 Introduction

Currently, managing various forms of identities to represent people on the web is crucial for secure service access and privacy. Today's connected systems often contain sensitive information; there is an increased need for adequate security and privacy support. We believe that capabilities of semantic technology can contribute to providing solutions to these problems. This paper is proposing such a solution which is expected to handle the identity management and privacy issues in business organizations. Each person possesses certain privileges to access resources based on the roles he/she plays in an organisation. To provide these services, we have formulated policies and rules to control access to resources such as project documents. These role-based policies need to be computer readable, which is achieved through a formal representation of a domain. Semantic technologies enable such a computer readable presentation, and are introduced here to handle the growing need of identity management and privacy support in corporate network.

2 Motivation

A project oriented working culture is a common scenario in a business environment. Projects are often set up across organizations, which limits the usability of company internal content management systems. Members in a project have certain roles and based on these roles they enjoy certain rights and privileges in a project. Role-based identity management can facilitate access control and privacy enhancement provisions for service access in a business project.

Having these aspects in mind, we have designed a use case scenario (Figure 1) targeting a business environment. A fictive project named UMTS Release 9 roll-out (Rel9) is created by Telenor and Ericsson. Telenor members in this project are György Kalman and Josef Noll, and Ericsson is represented by Erik Swansson. These members have their own supervisors in their parent companies. The project has resources like documents, deliverables, member details etc. With Josef Noll, Telenor has the project leader in the Rel9 project, while the others are ordinary project members. Visitors (example, Geir Egeland) are any persons from Telenor or Ericsson who are not members of the Rel9 project but want to know about the project. Based on the roles, members have differential rights to access project resources. For example, supervisors have the authority to read project documents and have visibility of project member details.

On the basis of this scenario, we have developed access control and privacy enhancement mechanism through roles, policy and rules using semantic web technology which will be discussed in detail in Section 5.

3 Semantics for Access Control

The significance of adding privacy-enhancing technologies (PET) in virtual networks is overwhelming [1], [2]. The project scenario (Section 2 and Figure 1) which is introduced in this paper is similar to a community in business environment having higher access control and privacy requirements. Not much research has focused on providing access control and privacy support in community environments involving semantic technology. Krug et al. provided a solution for community-aware identity management with access rights delegation [3], [4]. Instead of maintaining a centralised access control list, a trust based access right group has been proposed to delegate access rights. A private key based signature scheme was proposed to ensure the privacy of networks and users, which requires secure distribution and maintenance of keys. A similar concept of trust has been used by [5] to create and access community resources. A distributed trust management approach is also considered as one of the main components to secure the Semantic Web [6]. The authors intended to provide access to community and privacy solutions only by means of trust or reputation management; however, this does not provide adequate security in business contexts, which require a higher level of

ISSN 0085-7130

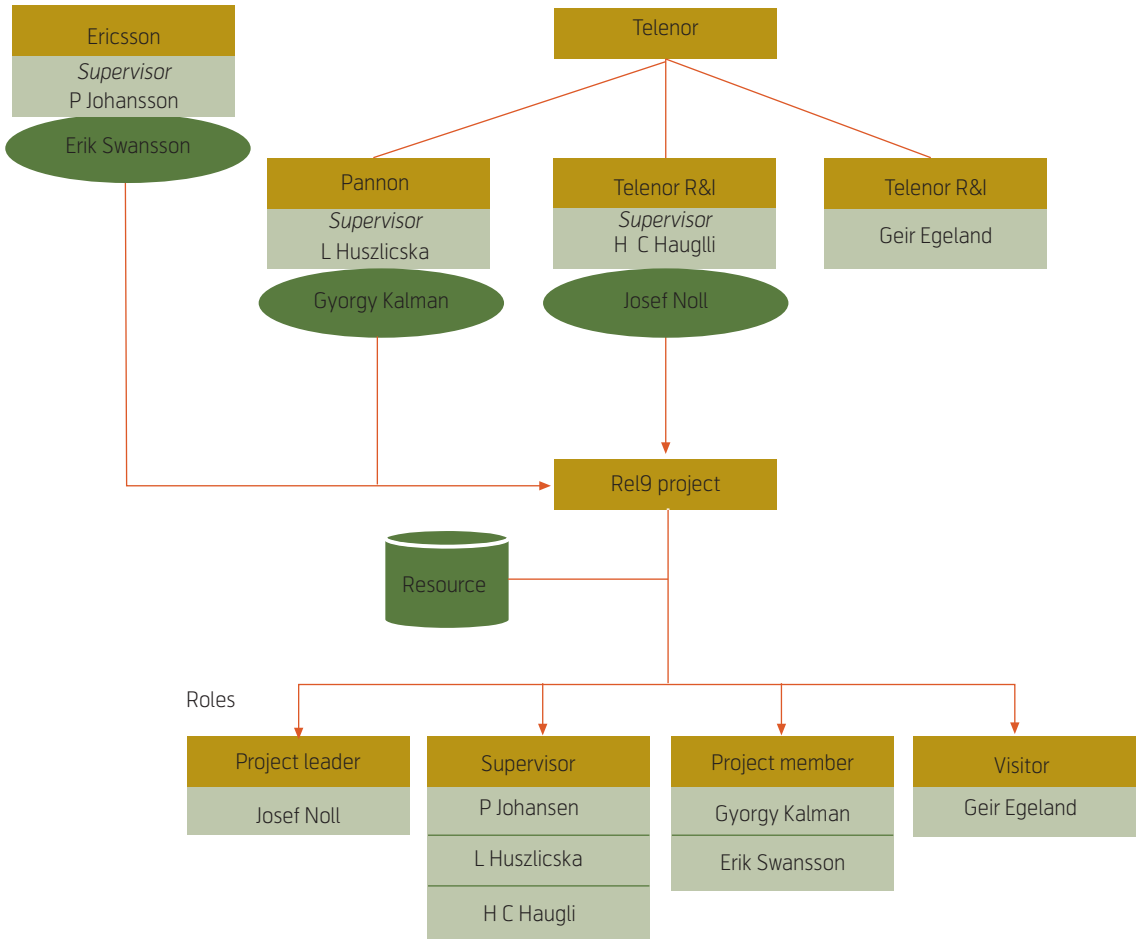

Figure 1 Use case scenario: Release 9 project

security. Trust is affected by various factors and therefore difficult to quantify.

FOAF (friend of a friend) was used by Krug et al. to delegate trust in a community [3]. Instead of FOAF, this paper uses the Web Ontology Language (OWL) which has more facilities for expressing meaning and semantics than FOAF. Finini proposed to use semantic languages such as OWL for constructing ontologies which define policies in [6]. In another paper [7], Smith introduced role-based access control (RBAC) policy management concepts. The National Aeronautics and Space Administration (NASA) uses semantic technologies like OWL to manage policies and access mechanisms across the organisation. Smith used the algorithms introduced by Kolovski [8]. Few of these concepts have been applied to express policies and rules such as those in our paper. To simplify access control, the Liberty Alliance Project[1)] introduced Circle-of-Trust (COT) to establish a legal framework for identity federation. But it lacks finer granularity of service access rights (based on differential access rights) and privacy. The notion of community-aware service access and privacy assurance can be addressed in a similar manner through the proposed architecture of this paper.

4 User, Device and Service Environment

This section focuses on the challenges of a ubiquitous service environment, supporting the preferences and context of the user and his communication devices.

4.1 Service Environment Scenario

Historically a service centric architecture was introduced to let services communicate with each other. The user- or I-centric approach, postulated by the Wireless World Research Forum (WWRF), is based on the transition of access delivery to service delivery [9]. Current rule-based algorithms become too complex when handling user context and preferences, thus asking for new mechanisms allowing dynamic adaptability of services.

The service centric world was introduced based on service level agreements (SLA) between trusted partners. In a more dynamic service provisioning world,

1) *Liberty Alliance Project, http://www.projectliberty.org/*

ISSN 0085-7130©Telenor ASA 2007

as envisaged in a Semantic Web Services environment, privacy becomes one of the key issues [10]. Our approach is to take advantage of the developments in both worlds, using the privacy and security mechanisms of the I-centric world and combining them with the semantic representation of data as known from the Semantic Web (Services) World [11].

The key challenge in a user-centric approach is the handling of user preferences, context, devices, and connectivity with proper privacy assurance required by these features. The European project ePerSpace introduced personal service delivery in the home segment, based on user profiles and preferences [12]. Experiences from this and similar projects showed that managing and updating preferences is a tedious work. While the home is a rather controlled environment, with trusted and known constellations of devices, the mobile world is more vulnerable. The ever increasing connectivity to the Internet with these mobile devices introduces various security and privacy threats. Service delivery in the mobile/wireless world is more complex. Louis V. Gerstner, Jr. of IBM said: *Picture a day when a billion people will interact with a million e-Businesses via a trillion interconnected, intelligent devices*. Pervasive systems do not just mean computers everywhere; it means computers, networks, applications, and services everywhere. To build personalised services is a challenge to the system design in pervasive environment from a security and privacy point of view.

Service access is coupled to user identity, or a way of proof that *I am the person who is allowed to access/ purchase the service*. Identity is verified through an authentication mechanism. Personalisation is based on handling the user's identity. Approaches for a mathematical description of identities have a long tradition. Khoshaflau claimed back in 1986 the need for a 'strong support of identity', and described identities through a graphical representation [13].

The introduction of semantics and the representation in .rdf and .xml allows describing user preferences and relations to characterise the roles of the users as indicated in the business use case scenario illustrated in Section 2.

4.2 Semantic Service Delivery

New methodologies, techniques and tools are necessary to develop and maintain services for the future that are attractive, easy to use and sufficently cheap. Concepts and technologies like Service Oriented Architectures (SOA), Web Services (WS), Semantic Web (SW) and Semantic Web Services (SWS) have gradually grown up to show their viability, especially if they are used in combination. Semantic Web-based technologies are widely acknowledged to play an important role in solving the interoperability problem between applications; the usage of semantic description in the context of advanced services delivery is expected to support easy access to the services. Not only do such formal and explicit descriptions enable easy service integration, but they will also support the exchange of preferences, profiles and context information of users.

According to the OASIS framework SOA is an architectural paradigm (model) that does not necessarily mean usage of Web Services, although Web Service is a popular implementation [14]. One prototypical implementation of a Semantic SOA platform was performed in the European Research project Adaptive Services Grid[2)] (ASG) in order to dynamically create services for the end user. While a technical implementation of a semantic service platform might be expected in the time frame 2009/2010, issues like privacy and protection of user requests and dynamic service level agreements between service providers might hamper the time to market [15]. Kagal et al. pointed out similar findings and claimed the necessity to extend Web Services in privacy and security [10]. They suggested extending Semantic Web Services with policies, representing security requirements for service discovery and privacy protection of user requests. These mechanisms of semantic technologies are used there to address privacy and security concerns in service delivery. We suggest extending the usage of semantic descriptions to user preferences and context, thus allowing to dismiss only the required information for a specific service request.

The mobile service world has made the move to a Web service oriented architecture. Noll et al. used a semantic annotation of advanced Telecom services to achieve exchange of roaming information on a dynamic basis [16]. The main findings of the approach were the cost reductions in service delivery, due to reduced effort for testing and updating of Web services in a semantic service world.

4.3 Authentication Mechanism

Extending the user preferences and context description in a semantic manner supports the disclosure of just the relevant user information for secure service access. In our scenario, access to Rel9 documents should only be granted to members and superiors of the Rel9 project. Today such access is often secured through directory access mechanisms which have limited functionality and are complex to manage.

2) *http://asg-platform.org*

ISSN 0085-7130

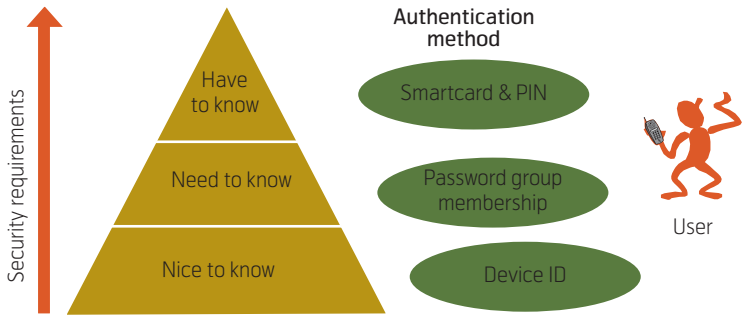

Figure 2 Security requirements for service access

Our approach is to define access rights through corporate relations, e.g. all superiors of Rel9 project members have read access to technical documents produced in the project. Depending on the security requirements of the specific service (see Figure 2), identification can be of type *nice to know*, e.g. using the device identity; *need to know,* through e.g. password, or *have to know,* through e.g. smartcard and pin code. Different identification mechanisms for the variety of services are defined and realise the mechanisms suggested by the Initiative for open authentication[3]; (i) SIM authentication (SIM), (ii) Public Key Infrastructure (PKI), and (iii) One-Time-Password (OTP).

The difference from today's authentication is that a person does not identify himself to a specific service, but is asked to verify his role (e.g. corporate relationship) providing him with the service access. Information about the user will not be disclosed; the service provider will just receive a certificate ensuring that the user has sufficient rights to use the service.

4.4 Mobile Supported Service World

Service access includes more and more the mobile phone, examples of which are admittance and payment services through contactless cards. Near Field Communications (NFC) enables these services on the mobile phone; the technology is prototyped worldwide, e.g. from MasterCard in Dallas [17]. One goal of these field trials is to demonstrate interworking between wireless technologies and NFC, another goal is to address security issues like potential threats as well as identity, privacy and simplicity. Adding NFC capabilities to the mobile phone opens for key exchange through near field and through the mobile network, thus providing a principle way of delivering authentication information. It is assumed that members of the company/project are authenticated through keys. These keys are distributed between the members using short messages (SMS) service or beforehand through NFC technology. This capability of in-band or out-of-band delivery of authentication keys makes the mobile phone a preferred device in administrating access rights.

5 Identity Management

A dynamic service request, taking into account the privacy requirements of a user, can be treated as identity administration. Identity is reputation: *what I say about me and what others say about me* [18]. My reputation is different, depending on whether I am at work, doing sports, or enjoying membership awards in a club. In the virtual world identity handling is more difficult, taking into account the dynamic service requests and privacy requirements of a user. Roccas introduced this in 2002 through the term social identity complexity, defining a new theoretical construct that refers to an individual's subjective representation of the interrelationships between his or her multiple group identities [19].

The Internet was built without an identity layer. In the current Web2.0[4] discussion Identity2.0[5] is introduced to interconnect people, information and software. Various institutes and industries are working to provide better identity management solutions. The Web community has defined Laws of Identity, providing a unifying identity meta-system that can offer the Internet the identity layer it needs [20]. It claims to handle minimal disclosure for Constrained Use, thus the claim to protect the privacy of the user. In Liberty Alliance[6], members are working to build federated identity and interoperability mechanisms in multiple federations. Within this, they are focusing on end user privacy and confidentiality issues and solutions against identity theft. Another solution, Sxip[7] has been designed to address the user-centric identity architecture. It provides user identification, authentication and internet form fill solutions using web interfaces for storing user identity, attribute profiles and facilitating automatic exchange of identity data over the Internet. To access online services, Windows CardSpace[8] uses various virtual cards (mimic physi-

3) *OATH, http://www.openauthentication.org/*
4) *http://en.wikipedia.org/wiki/Web_2*
5) *http://identity20.com/media/OSCON2005/*
6) *http://www.projectliberty.org/*
7) *http://www.sxip.com/*
8) *http://cardspace.netfx3.com/*

ISSN 0085-7130©Telenor ASA 2007

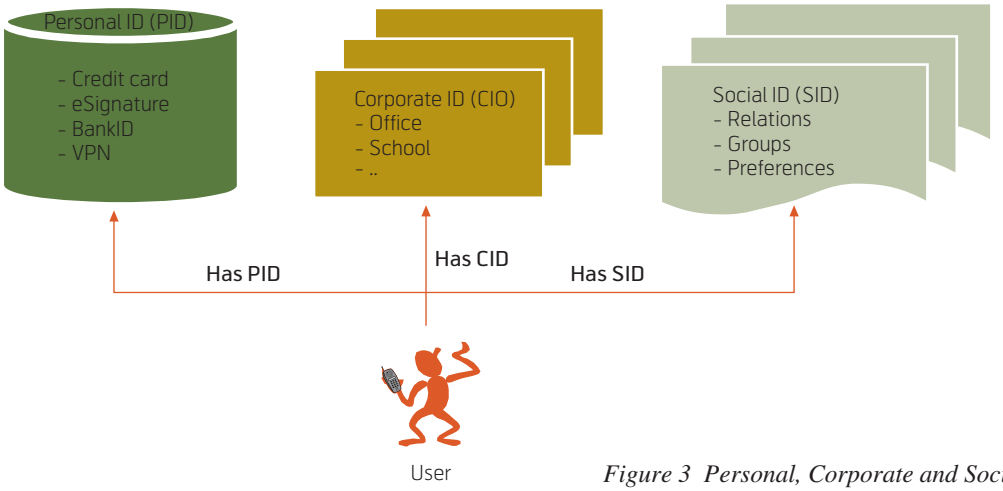

Figure 3 Personal, Corporate and Social Identities

cal cards) issued by the identity providers for user identifications and authentication, each retrieving identity data from an identity provider in a secure manner.

Most of these mechanisms are tailored to foster the usage of identity based web services. Our scheme focuses on the identity management in business community based on the relationships of its actors with the community facilitating the access to its contents and privacy enhancement.

5.1 Representing Identity

The proposed integrated identity mechanism consists of certificates, keys and preferences stored in a personal device and in the network. These identities are categorized in three groups of identity; personal identity (PID), corporate identity (CID) and social identity (SID), based on the roles exercised by a person in real life [21]. Figure 3 shows example applications of PID, CID and SID.

Our approach suggests a decentralised identity architecture, consisting of network components and the personal device of the user. Such an approach brings the user in control of his services, allowing him to accept or deny access to privacy information. The mechanism builds on a personal user device, typically a mobile phone, providing the underlying infrastructure. With the identity subscription certificate users can access the network identity repository, e.g. service references located in the SID. Identities stored in this repository can give access to services (remote or proximity) that need medium or low level of security requirements. The main reason to store service and user preferences in the network is the availability of the network repository and the short response time, avoiding the costly and varying mobile/wireless link. Personal identities (PID) require high security, and will thus be stored in the personal device of the user, allowing him to control when and what PID information is released to service providers.

Semantic Web technology is proposed to represent role-based identity management in areas of business/social resource access.

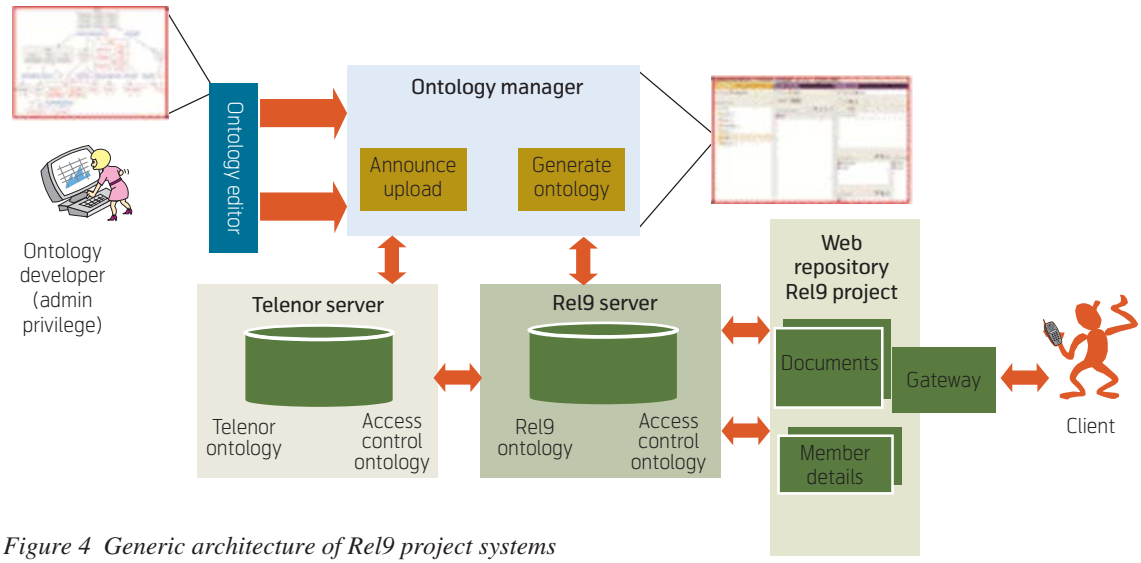

Figure 4 Generic architecture of Rel9 project systems

ISSN 0085-7130©Telenor ASA 2007

5.2 Generic Architecture of the System

Users are authenticated by the identity providers of corporate organisations using keys. These keys are assumed distributed only among the members of the company/project using the mobile environment or near-field communications. They then access the company/project contents using the proposed role-based ontology with differential access rights. The generic architecture of this paper is illustrated in Figure 4. The project membership and access rights management to the project contents is handled through a project ontology. While the project ontology handles the project members' access to content, the company ontology will allow the supervisors of project members to do so. Our service scenario builds on the relationship between the actors and establishes access rights to content.

5.3 Role-based Identity Management

A business project group is composed of several different types of project members. They can be categorized based on the roles they play in the project. Each of the roles has different privileges or rights to access different project resources. Table 1 shows examples of such scenarios. Access control to project resources and maintaining privacy of project member information are the objectives of the proposed ontology. 'He is leader of the Rel9 project' refers to his corporate identity (CID) in professional life and his role in the Rel9 project. The project leader has administrative and final approval privileges which the project members do not have. One of the crucial requirements of privacy is to ensure that a visitor should not be allowed to see the project member details (for example; contact address, email, phone number, etc.). Project leader and members have visibility of member details. Project members (including project leader) have their own supervisors in parent organizations. Supervisors may want to know about project status, see (or even write) project documents, deliverables and member details. The role as supervisors ensures these features.

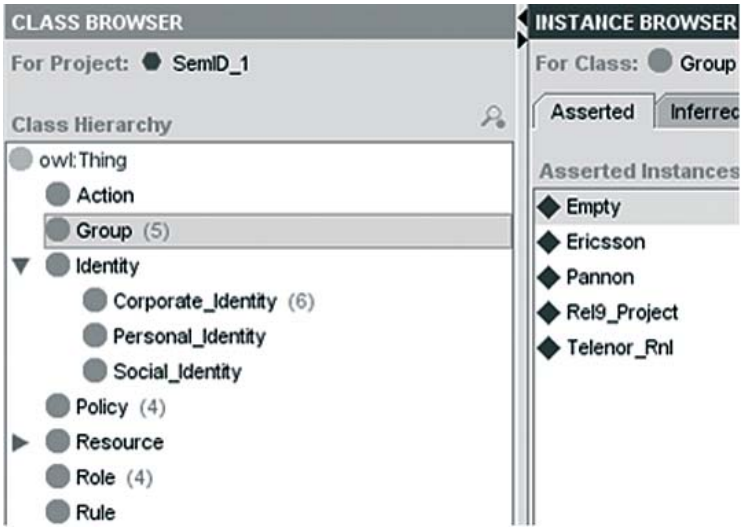

Figure 5 Classes and subclasses of ontology

Figure 1 of Section 2 illustrated our use case scenario. The Semantic Identity Management (SemID.org) ontology has been developed based on this scenario.

5.3.1 Policy and Rule

The corporate identity of each project member, the project group to which he belongs and the role he plays are defined in the ontology. Each role has certain policy (or policies). A policy (P) represents the privilege reserved for each role in a community and expressed through a set of rules (R_1, R_2, ..., R_n). Therefore a policy can be presented as

$$P = \{R_1, R_2, ..., R_n\}.$$

A rule is a function that takes an access request as input and results in an action (permit, deny or not-applicable). A rule is composed of the triple Subject (S), Resource (R) and Action (A) that must be met for a rule to apply to a given request. In the proposed SemID ontology, Subjects are the identities that play specific Roles (which is predefined in the ontology) like project leader, supervisor, project member and visitor. Resources are the project resources like deliverables, documents, etc. So, the rule is simplified as

$$R = \{S, R, A\}.$$

If Josef Noll is the project leader and he wants to write over a project deliverable, the corresponding rule will be defined as

$$R = \{ProjectLeader, Deliverables, Submit\}.$$

For the same purpose, the corresponding rule of the visitor Geir Egeland will be defined as

$$R = \{Visitor, Deliverables, Deny\}.$$

These example rules belong to the policy: *write*. However, these access control rules have not been explicitly defined in the modelled ontology which will be implemented in later works. It is assumed that relevant subjects (individuals defined as CIDs in the ontology) are going to be authenticated to their company systems through secure means. In our case it

9) *Protégé, http://protege.stanford.edu/*

ISSN 0085-7130©Telenor ASA 2007

means that Geir Egeland is authenticated as Telenor R&I member, which through Telenor's participation in Rel9 gives him guest status in the Rel9 project.

In conclusion, access control to project resources is maintained through policies and rules.

5.3.2 Ontology of the System

We model the ontology of the use case scenario with OWL-DL using the Protégé ontology editor platform[9]. In the left part of Figure 5 classes and subclasses of the SemID ontology are presented, modelling the proposed use case and meeting the requirements. Figure 5 also illustrates the instances of four different groups described in the use case scenario. An *empty* group has been created to support privacy of a group when visitors try to access resources.

In this ontology, the corporate identity (CID) of each representative is defined by corresponding names. These are the instances of Identity subclass: CID. Anyone whose Identity instance is not defined explicitly in SemID will be considered as 'Visitor'. Each instance has four properties: *hasGroup*, *hasVisibility*, *hasRole* and *hasSupervisor*. The group to which a member belongs is explicitly identified using *hasGroup* property. *hasVisibility* points to the groups a member needs general purpose visibility to. The Role a person plays in a project is identified by *hasRole*. *hasSupervisor* explicitly defines 'who is supervisor of whom'. Example source codes (RDF/XML) of corporate identities and their properties are as follows:

```
<Corporate_Identity rdf:ID=
"Erik_Swansson">
  <hasGroup rdf:resource="#Ericsson"/>
  <hasGroup rdf:resource="#Rel9_
  Project"/>
  <hasVisibility rdf:resource=
  "#Ericsson"/>
  <hasVisibility rdf:resource=
  "#Rel9_Project"/>
  <hasRole rdf:resource=
  "#Project_Member"/>
  <hasSupervisor
rdf:resource="#Peter_Johansson"/>
</Corporate_Identity>
```

There are four possible roles in the Rel9 project. Each Role has specific policy/policies. These are expressed by *hasPolicy* property. The following source code illustrates four different policies of these roles: Administrator, FinalApproval, Read and ReadWrite. Administrator policy is introduced to represent the administrative privilege of the project leader and similarly, FinalApproval policy refers to the final approval of project deliverables.

Project roles	Privileges	Project resources
Project leader	Administrator	Membership details
	Final Approval	Deliverables
	Read/Write	Documents
	Visibility	Member details
Supervisors	Read/Write	Deliverables
		Documents
	Visibility	Member details
Members	Read/Write	Documents
	Visibility	Member details
Visitors	Read only	Documents
	No visibility	Member details

Table 1 Roles in a project and their privileges to access resources

```
<Policy rdf:ID="Administrator"/>
  <Policy rdf:ID="FinalApproval"/>
  <Policy rdf:ID="Read"/>
  <Policy rdf:ID="ReadWrite"/>
```

Four different roles of the project are represented by four instances of Role: Project leader, Supervisor, Project member, and Visitor. Appropriate policies are added to each instance of Role. According to the use case scenario, the project leader has the policies: *Administrator*, *FinalApproval* and *ReadWrite*. 'Visibility' privilege deals with the privacy of the project and is satisfied through two properties: *hasVisibility* and *hasVisibilityOfGroup*. In order to fulfill the requirements of group member's privacy, a *hasVisibilityOfGroup* property has been created. The Visitor instance has visibility of group called '*empty*' (an instance of class: Group) to ensure that 'as a visitor one should be allowed to read the documents of the project, but he does not have the permission to see the member details of the visited project'. Example codes to represent roles and corresponding properties in the ontology are as follows:

```
<Role rdf:ID="Project_Leader">
  <hasVisibilityOfGroup
rdf:resource="#Rel9_Project"/>
  <hasPolicy rdf:resource="#Administrator"/>
  <hasPolicy rdf:resource="#Final Approval"/>
  <hasPolicy rdf:resource="#ReadWrite"/>
</Role>
```

In this ontology, we have defined ten properties. Each property has its domain and range. The classes to which a property is attached are called domain. Allowed classes for properties are often called a range of a property. Sample source codes of the implementation of these properties and corresponding domain and range are given as follows:

ISSN 0085-7130

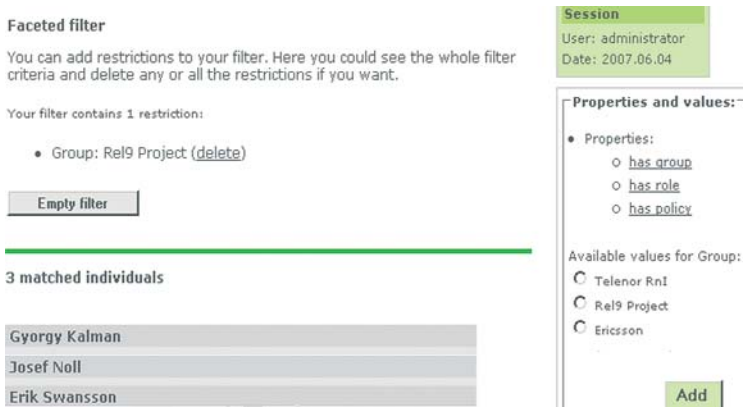

Figure 6 Screen shot of SEDO for users with administrative rights

```
<owl:ObjectProperty rdf:ID="hasAction">
  <rdfs:domain rdf:resource="#Rule"/>
  <rdfs:range rdf:resource="#Action"/>
</owl:ObjectProperty>
  ……..
<owl:ObjectProperty rdf:ID="hasGroup">
  <rdfs:domain rdf:resource="#Identity"/>
  <rdfs:domain rdf:resource="#Group"/>
</owl:ObjectProperty>
```

hasVisibility and *hasVisibilityOfGroup* ensure the privacy of groups. *hasSubject*, *hasResource* and *hasAction* create the simplified rule.

5.3.3 Privacy Enhancement

Privacy requirements are satisfied in the SemID ontology using two properties (*hasVisibility* and *hasVisibilityOfGroup*). *hasVisibilityOfGroup* is attached to class: Role and *hasVisibility* are attached to class: Identity (subclass: CID). The latter is rather a general visibility property which ensures that anyone belonging to at least one group has visibility of resources of those groups. Role based visibility (*hasVisibilityOfGroup*) represents the visibility of specific resources like the project member details. Leader, members and supervisors of the Rel9 project have visibility of project members' details which the visitors cannot see. This privacy feature is introduced to protect member details, such as email and phone number to visitors. We introduced the role of supervisor in order to satisfy the information requirements of participating companies, namely Telenor and Ericsson. Supervisors have access to member details, ensured through SemID.

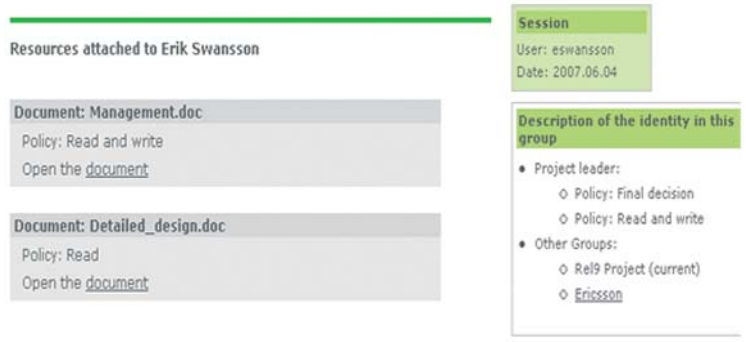

Figure 7 Screen shot of the SEDO software when the user is logged-in as normal project member

6 Semantic-based Enterprise Content Management

The ontology developed above was integrated by Universidad Carlos III de Madrid in SEDO, a Semantics-based Enterprise Content Management System [22]. In a nutshell, an Enterprise Content Management System (ECMS) is a software application used to manage computer files, media, audio files, electronic documents and web content inside the boundaries of a company, specifying different levels of access for those business resources. The idea behind the ECMS is to make these files available both within the company as well as over the web. Figures 6 and 7 show screen shots of the implemented software.

SEDO is implemented by means of Ruby on Rails (RoR)[10]. The SemID ontology has been used as a conceptual backbone for the permissions and access levels of the different users of the system. There are a number of things that can be achieved by the SEDO system thanks to the conceptual backbone of the SemID ontology and they are summarised as follows:

- *Creating and annotating resources and SEDO users*

Semantic descriptions are added to the resources, together with a number of rules and policies. The description is formalised through the SemID ontology.

- *Navigating and Searching through semantics*

Filtering the information depending on the properties of the ontology is what is called "Faceted Search and Browsing" [23]. In a nutshell, facets are orthogonal conceptual dimensions of the data, and SEDO allows us to see, for example, which other users are eligible to access a particular resource like "Document 1" of the Rel9 project.

7 Conclusion

This paper addresses the complexity of content handling in projects involving multiple organisations. Project content is typically stored within one company system, making it difficult to share the content across company borders.

[10] *Ruby on Rails, http://www.rubyonrails.org*

ISSN 0085-7130©Telenor ASA 2007

We introduced semantic technologies to describe in a formal way the roles and corresponding access policies. Roles and access rights for project members and their superiors in the parent companies are formalised in the Semantic Identity (SemID.org) ontology.

The prototypical implementation in a semantic-based enterprise content management system demonstrates the capabilities of the approach. An identity management based on roles represents a flexible, efficient and secure way to ensure that only relevant content is dissolved.

References

1 Chewar, C M, McCrickard, D S, Carroll, J M. *Persistent virtual identity in community networks: Impact to social capital value chains*. Virginia Tech, Computer Science, 2003. (Technical Report TR-03-01)

2 Walters, G J. Privacy and Security: An Ethical Analysis. *Computers and Society*, 2001, 8-23.

3 Kruk, S R, Grzonkowski, S, Gzella, A, Woroniecki, T, Choi, H-C. D-FOAF: Distributed Identity Management with Access Roghts Delegation. *1st Asian Semantic Web Conference*, Beijing, China, 2006.

4 Kruk, S R, Gzella, A, Grzonkowski, S. *D-FOAF Distributed Identity Management based on Social Networks*. In demo session of ESWC 2006.

5 Choi, H-C et al. Trust Models for Community-Aware Identity Management. *Identity, Reference and the Web IRW2006. WWW2006 Workshop*, Scotland, May 23, 2006.

6 Finin, T, Joshi, A. Agents, Trust, and Information Access on the Semantic Web. *ACM SIGMOD*, 31 (4), 30-35, 2002. (Special Issue: Special section on semantic web and data management)

7 Smith, M A et al. Mother, May I? OWL-based Policy Management at NASA. *European Semantic Web Conference 2007, ESWC2007*.

8 Kolovski, V, Hendler, J, Parsia, B. Analyzing Web Access Control Policies. *16th International World Wide Web Conference, WWW2007*, Alberta, Canada, May 8-12, 2007.

9 Kellerer, W et al. *Systems beyond 3G – Operators' vision*. Eurescom Project P1203, December 2002.

10 Kagal, L et al. Authorization and Privacy for Semantic Web Services. *IEEE Int. Systems*, 19 (4), 50-56, 2004.

11 McIlraith, S A, Cao Son, T, Zeng, H. Semantic Web Services. *IEEE Int. Systems*, 16 (2), 46-53, 2001.

12 Danet, P Y. ePerSpace: A European Project for the Seamless and Personalised Digital Communicating Home of the Future. *European VPN Services Forum Conference*, London, June 15-17, 2006.

13 Khoshaflau, S N, Copeland, G P. Object Identity. *Proceedings OOPSLA'86*, Sept. 1986, 406-416.

14 MacKenzie, C M et al. OASIS, Reference Model for Service Oriented Architectures 1.0. August 2, 2006. January 10, 2007 [online] – URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev= soa-rm

15 Noll, J, Lillevold, E. Roadmap to ASG based Semantic Web Services. In: *Proc. of The International Conference on Internet & Web Applications and Services 2006, ICIW*, February 23-25, 2006.

16 Noll, J et al. Estimating business profitability of Semantic Web Services for Mobile Users. In: Schaffert, S, Sure, Y. *Semantic Systems, From Visions to Applications, Proc. of the Semantics 2006*. Österreichische Computer Gesellschaft, 195-204.

17 Cellular-news. *MasterCard Tests NFC Payments with Nokia Handsets*. December 10, 2006 [online] – URL: http://www.cellular-news.com/story/20211.php

18 Hardt, D. Identity 2.0. *OSCON 2005*. November 2, 2007 [online] – URL: http://www.identity20.com/media/OSCON2005/

19 Roccas, S, Brewer, M B. Social Identity Complexity. *Personality and Social Psychology Review*, 6 (2), 88-106, 2002.

20 *The Laws of Identity*. October 11, 2007 [online] – URL: http://www.identityblog.com/stories/2004/12/09/thelaws.html

21 Chowdhury, M M R, Noll, J. Distributed Identity for Secure Service Interaction. P*roc. Third Intern. Conference on Wireless and Mobile Communica-*

ISSN 0085-7130©Telenor ASA 2007

tions, ICWMC07, Gouadeloupe, French Caribbean, March 4-9, 2007

22 Chowdhury, M M R, Gomez, J M, Noll, J, Crespo, A G. SemID: Combining Semantics with Identity Management. *Intern. Conf. on Emerging Security Information, Systems and Technologies, SECURWARE 2007*, Valencia, Spain, October 2007.

23 Oren, E et al. (2007, May). Activerdf: Object-oriented semantic web programming. In: *WWW '07: Proceedings of the 16th international conference on World Wide Web*, Banff, Alberta, Canada, May 2007, 817-824. New York, NY, ACM Press.

Mohammad M.R. Chowdhury is a PhD student at the University Graduate Center at Kjeller (UniK), Norway, in the area of User Mobility and Service Continuity. He received his MSc from Helsinki University of Technology in Radio Communication. Before joining his current position, he was radio planning engineer at GrameenPhone, a Telenor subsidiary in Bangladesh.
His current areas of interest are identity, identity representations and identity based service interactions, seamless user experience in heterogeneous wireless networks and development of innovative service concepts for mobile.

email: mohammad@unik.no

Josef Noll holds a professor stipend from the University of Oslo in the area of Mobile Services. Working areas include Mobile Authentication, Wireless Broadband Access, Personalised Services, Mobile-Fixed Integration and the Evolution to 4G systems. He is also Senior Adviser in Movation, Norway's leading innovation company for mobile services.
Previously, he was Senior Adviser in Telenor R&I in the Products and Markets group, and was use-case leader in the EU FP6 'Adaptive Services Grid (ASG)' projects, and has initiated i.a. the EU's 6th FP ePerSpace and several Eurescom projects.

email: josef@unik.no

ISSN 0085-7130©Telenor ASA 2007