Semantic Policies for Service Access in Mobile supported Sensor Networks

Sarfraz Alam, Josef Noll, *Member, IEEE,* and Dumitru Roman

***Abstract*—This paper addresses issues of service access, and policies to control access to these services. It introduces the mobile phone as a service aggregator and control centre for sensor networks. Semantic policies are used to extend the encryption-based radio link protection by an application layer protection. Two scenarios are introduced, covering home access and content access in the home. The implementation of key elements such as mobile-based key distribution and semantic-based policies are performed in order to show the feasibility of the approach.**

***Index Terms*—Sensor network, Access policies, Privacy, Service Oriented Architecture, Policies, Semantics**

I. Introduction

WEB 2.0 also known as The Social Web not only revolutionized the front end of the Web but also changed the way of interaction between people. Different social networks and blogs are used to share the information and content. Current developments in the Web 3.0 initiatives have focus on the backend of the Web to reengineer the underlying technologies of the Web for making sense of information. The smart capabilities of the Web spur us to envision the future web as Web of services rather than web of things.

The envisage Web of Services concept comprises of Internet and Mobile services that are adaptive towards the individual preferences. The increase in service offering through the Internet and mobile network will make the mobile devices a key tool for service access in digital environment. Technology advancements have enhanced the capabilities of mobile devices in recent years but still mobile service provision is hampered from the limited capabilities of mobile phones. The need of service personalization, including adaption of individual preferences, terminal and network capabilities requires advanced service capabilities, especially openness of interfaces on the mobile phone. Willingness of use and access services from anywhere at any time that congener individual preferences put each individual in the driving position. The need of an I-Centric approach with perceive control is the identified challenge to tackle personalised mobile service provisioning [1].

The main challenge with today's mobile world is the segregation of both mobile/proximity and Internet services. A mobile device is typically in a dynamically changing service environment, which makes the integration of mobile/proximity and Internet services difficult. In this paper we propose the concept of a virtual mobile that together with the real device and the surrounding sensors can work as the integrator of these service worlds. The virtual mobile will also open for service composition including context and user preferences. A new mobile web services architecture is proposed, consisting of a semantic service repository, handling both Internet and mobile/proximity services.

The paper is structured as follows: Section II provides details on the user-centric service approach, and section III will introduce device enriched context. Section IV outlines the extended mobile and sensor WS architecure, and section V provides the proof-of-concept through implementation of key elements. Ideas for future work will conclude the paper.

II. User-centric service approach

In the digital world the user is often represented through a role-based identity [2]. Authentication can be provided through the mobile phone, which is expected to be in the hands of 4 billion people by the end of 2009. Developments of near-field communication (NFC)[1] for payment and access, provisioning of one-time-password (OTP) and other authentication methods are assumed to be the dominant mobile developments in 2009/2010 [3]. Thus we expect that the mobile phone will become the device providing the role-based identity and connectivity to services in the user's surrounding and the Internet.

Currently the mobile service world can be categorized as addressing mobile services, Internet services and proximity services from the mobile device. Mobile services are typically native services in a mobile device, examples of which are phone and SMS services, and device hosted services where mobile device offers services to the other service provider. Internet services are usually ecommerce and m-commerce services and proximity services are the services in the vicinity of the user such as payment, access and admittance.

This service world is illustrated in figure 1. To cope with the highly complex mobile service world new technology enablers both in the handset and the mobile networks are required that enable development of next generation mobile services. Concepts and technologies like Service Oriented Architecture (SOA), Web Services (WS), Semantic Web (SW) and Semantic Web Services (SWS) have gradually grown up to show their viability [4]. The mobile service world has already made the move to SOA and is poised to take advantages of interoperability provided by web services. Most of the

J. Noll, member of IEEE, is professor at the University of Oslo (UiO) and the University Graduate Center (UNIK), 2027 Kjeller, Norway (email: josef.noll@unik.no).

Sarfraz Alam is PhD researcher at UNIK (e-mail:sarfraz@unik.no).

Dumitru Roman is researcher at the STI institute in Innsbruck, Austria (e-mail: dumitru.roman@sti2.at)

Manuscript received May 23, 2008. This work was supported in part by the Norwegian Research Council and ITEA through the WellCom project.

[1] Near-field communication, http://www.nfc-forum.org

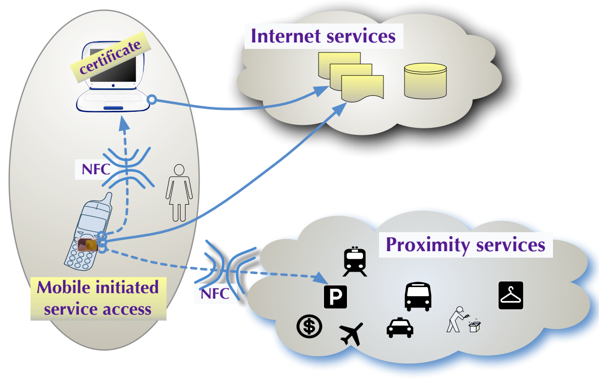

Fig. 1. Mobile and Internet Service World

mobile services like location information are available through ParlayX Web service interfaces[2].

The usage of semantic annotation in the context of advanced services delivery is expected to support easy access to the services and improve the inherit flexibility of SOA. Not only formal and explicit descriptions enable easy service integration, but they also support exchange of preferences, profile and context information of mobile users. This paper suggests to extend the mobile SOA world by integrating services from sensors, thus allowing semantic service composition of sensor, mobile and Internet services.

III. Device enriched context

With the recent development of mobile and sensor technology a considerable urge and rise is seen in building mobile context aware services. Sensors are playing a crucial role in context aware services and act as context aware supporter for mobile device. Context sensing can be either internal where the mobile device has an embedded sensor or external where the mobile device acquires context information from the external sensors or sensor networks. Technology advancements enable the mobile phone to offer various services in many different scenarios due to its communication and interface capabilities.

We envisage the use of the mobile device as context provider to other services, personalized service aggregator and service provider (SPn). The concept is depicted in the figure 2, where each mobile phone can act as service aggregator. It enables both proximity and mobile services and acts as a gateway to sensors and sensor networks.

A. Use of Semantic Web Technology

Maturity of semantic web technologies converge/advocates the mobile service world towards semantic enriched context aware services. In semantic enriched context aware systems, the mobile device typically acquires context from the sensors or other mobile devices. This context information is combined with the context ontology and then stored in the knowledge-base. Later context reasoning is performed to find additional semantic relationship on the knowledge base in order to deliver

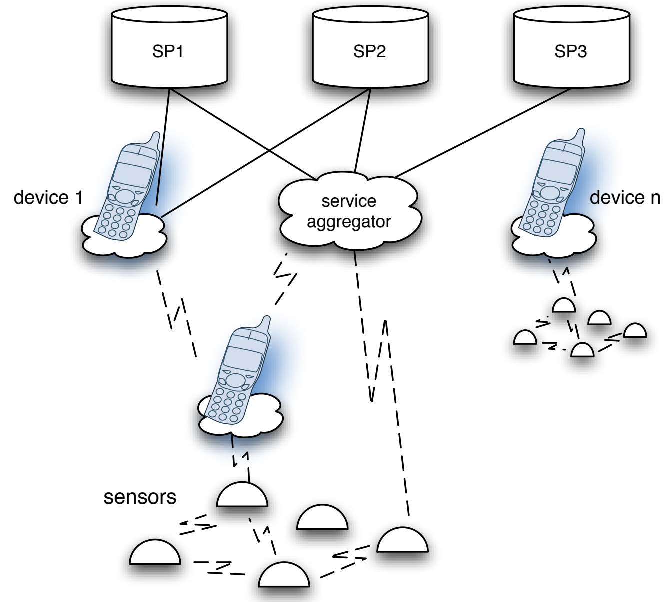

Fig. 2. Layered approach for mobile controlled sensor network

personalized service and content that is adaptive, tailored and appropriate to the device capabilities and context. Gu et. al. proposed an ontology based mobile framework with context reasoning capabilities [5]. The main components of the system are RDF/OWL parser, model extractor, sRDQL (a subset of SPARQL), reasoning engine and context repository. The main finding of the work was that the mobile devices are capable enough performing computing for semantic context aware services.

Realising web services on mobile devices is supported by all major mobile application development platforms such as Nokia Web services framework, S60, UiQ, Java ME, and .Net compact framework. A sketch of a Web Services enabled mobile phone is shown in figure 3, indicating both service registry, request and execution implemented on the device.

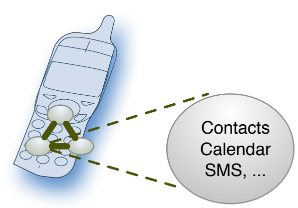

Fig. 3. Web Service Enabled Mobile Phone

B. Mobile phone as service aggregator

There exist a number of issues and challenges for Mobile SOA service provision, mainly because wireless and mobile networks are based on an unreliable radio transmission[3] [6]. Handling the service registry in the mobile phone is the dominating challenge. The unreliable radio, round-trip-delay

[2]The Parlay Group website, http://www.parlay.org

[3]Latency in Mobile Systems[6]: GPRS (~700ms), EDGE (350ms-600ms),WCDMA (200-300ms), HSDPA (~150ms)

and cost of air-time make interworking with a mobile-based service registry impractical. This paper suggests moving the service registry of sensor services, mobile and proximity services into a Web based service registry. Our envisaged future mobile is a set of services noted through the terminology virtual mobile. A virtual mobile integrates various user devices and both mobile/proximity and Internet services [7]. We use the concept of a virtual mobile to define service integration across platforms [8].

Introducing such a virtual mobile brings a number of advantages:

- *Security will be increased*, as the devices and services of the user are not visible to the outside world. Only services capabilities might be announced in the service repository of the virtual mobile.
- *Handling of communication according to the user preferences:* The user might define that after working hour calls from office colleague are transferred directly to the answering machine.
- *Integration of the context into dynamic service delivery*. As the virtual mobile can cache context information (location, presence, and identity), this information can easily be integrated into the service composition process.

Our approach is based on semantic technologies, details are discussed in section V.

C. Applicability in the home

We envisage the home as one of the areas where semantic policies for service access can be applied. Two scenarios are selected, covering *(i)* the physical access to the home and *(ii)* the access to content in the home. A user's mobile phone in the home can act as a mobile gateway in order to control the environment and stand-alone sensor networks that can provide context information, security settings and service information.

The home door lock is NFC supported and equipped with a control sensor to open and close the lock. In order to access the home the visitor needs a mobile key (mkey) that is sent to him by the house owner via SMS as an application [10]. The key is bind with a specified key ID, day, time and period, so that only the person with a valid key can access the home.

The second scenario addressing home content access is based on the ITEA WellCom project[4]. The scenario enables access to home entertainment such as TV and set top box (STB), and establishes context-aware services. The WellCom environment, depicted in figure 4, allows adaptation of services related to the consumed content, the user's preferences and her social environment.

Having entered the house the visitor needs to authenticate himself towards the STB. Depending on his relation to the house owner, her age or user-defined policies, the visitor may access content, use recoded content and access WellCom services. Details of the policies used here are addressed in section V-C.

[4]ITEA WellCom, http://www.itea-wellcom.org/

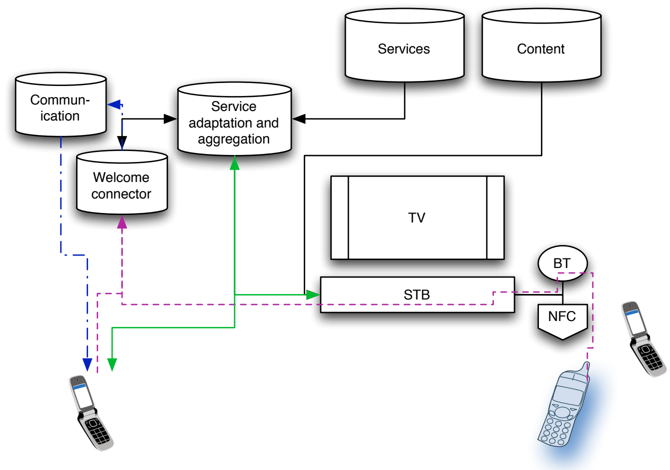

Fig. 4. Content and service access from users - ITEA-WellCom scenario

IV. Mobile and Sensor WS architecture

This section will provide the guideline for enabling I-centric service surrounding. It will also describe the mobile and sensor extended WS architecture with its main functionalities.

A. Enabling I-centric service surrounding

Elements of an I-centric service surrounding are *(i)* user representation using profiles, *(ii)* device representation, and *(iii)* service representation. We suggest using ontologies to integrate the various aspects. A policy engine will then take into account access control and privacy issues. Current security schemes for sensors and devices have often only a physical encryption of the radio link. Once this encryption (e.g. WEP, WPA) is cracked there is no restriction to service usage in the network or from the sensors.

We favour a two layer approach where we suggest "open world reasoning" for connectivity of devices, and "close world service access" for service usage from these devices. Our approach assumes that devices are visible, but access to the services on the devices is restricted through policies.

This *I-centric security scheme* enables QoS control in content access and communication, including parameters such as relevance, battery lifetime, processing power, and privacy.

B. Key functionalities

The proposed mobile web services architecture is extended by a new intelligent service registry as indicated in figure 5. In addition to the mobile phone representation, the virtual mobile has a semantic layer to handle semantically enabled mobile services. The availability of the semantic web service interfaces of sensor, mobile, and proximity services into the Internet service world opens for a new dimension of reasoning and service composition.

The architecture is based on the following key functionalities:

- The mobile phone as service aggregator,
- Semantic service profiles for devices,
- User profile ontology,

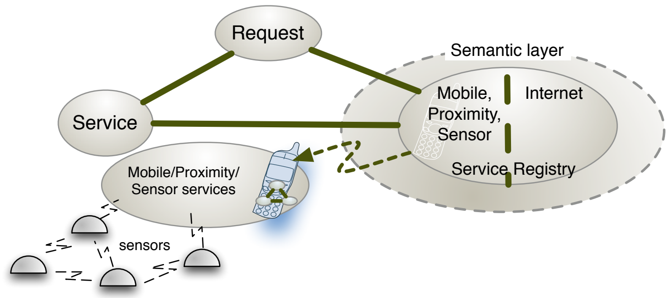

Fig. 5. Mobile and Sensor WS Architecture with Virtual Mobile in Repository

- Radio and application access (key distribution), and
- Policy engine for advanced reasoning.

Our approach provides a policy supported communication through the virtual mobile, using proxy-based or regular WS-communication. The implementation of policy-based access control is discussed later on.

Limited resources such as CPU, battery and radio are the biggest barrier when enabling mobile semantic web services for mobile terminals [5]. A virtual mobile in the network has no such limitations and can thus play the role of a semantic web execution environment. The virtual mobile can handle ontology storage, ontology processing, querying and reasoning. In a context aware service world systems consist of sensing, thinking and acting sub systems. The real mobile device is just acting as a context watcher/collector and thinking and acting will be performed in the virtual mobile. Thus performance issues are solved. With the help of a virtual mobile context aware service delivery is established and might incorporate highly personalised service delivery.

Policy-based access control can be enrolled to tackle the issue of authorised use of services.

V. Implementation of key elements

The following sections will provide the detail of proof-of-concept prototypical implementation of semantic service profile, key distribution and semantic policy engine.

A. Semantic Service profile

Studies by Indulska et. al. [9] have pointed out the needs of semantically enhanced profiles for user, device and service profiles. We suggest extending the Wireless Universal Resource File (WURFL[5]) for the device profile and 3GPP's Generic User Profile (GUP[6]) for the user profile.

WURFL is a promising approach to overcome practical issues related to device profiles. CC/PP[7] and UAProf[8] are not always accurately presented, and new capabilities require new vocabularies outside of CC/PP and UAProf. WURFL is an XML file that containes information on every known device in the WURFL community. The main attraction of this approach is that devices are arranged in an inheritance hierarchy that helps in inferring sensible defaults. But WURFL lacks information about the network, the software and the user preferences.

3GPP GUP is an ongoing effort to define a generic user profile. GUP is composed of a number of user profile components i.e. user, services, and user devices. Its main objective is to provide a way to enable harmonised usage of user related information located in different entities. Both GUP and WURFL are based on XML and XML schema, thus need to be ported into ontologies.

To illustrate the envisaged service profile of a virtual mobile we use the OWL DL code snippet of service profiles. The code describes the capabilities of SMS as follows: SMS contains text only and the number of characters in an SMS limits to 160.

```
<rdf:RDF xmlns
    /* namespaces are here */>
    ....
    <owl:DatatypeProperty rdf:ID="hasCharacter">
        <rdfs:domain rdf:resource="#Service"/>
        <rdfs:range rdf:resource="&xsd;int"/>
        <rdfs:comment rdf:datatype=
        "&xsd;string">160characters
        </rdfs:comment>
    </owl:DatatypeProperty>
    ....
    ....
    <owl:Class rdf:ID="Service"/>
    <Service rdf:ID="SMS">
        <hasSize rdf:datatype="&xsd;int">
        1120</hasSize>
        <hasCharacter rdf:datatype=
        "&xsd;int">160</hasCharacter>
        <contains rdf:resource="#Text"/>
    </Service>
    .....
</rdf:RDF>
```

Such a service description together with the device capabilities, a user profile and a context description will allow the provision of highly-adopted personalised services. While the above code snippet explains the profile of service on the mobile and on sensors, we envisage device profiles as e.g. WURFL to establish the device capabilities.

Example of *user profile ontologies*, which describe the preferences of the user, and which can be extended to a full user profile can be found at the University of Maryland[9] or others.

B. Key distribution for radio and application access

Key distribution necessary for accessing the home is used as an example on how device profiles are used to express the service capabilities of the devices. If the house owner wants to give access to a visitor, he will send an invitation to the service centre by using the person's nickname, mobile number, or another identifier. The semantic policy server checks that the visitor is in the house owner's friend list or community using the house owner's user and community profile (i.e. an ontology). If the visitor is in the list, the policy server will send the access key (mkey) allowing access the house. If the

[5]WURFL; http://wurfl.sourceforge.net/

[6]3GPP GUP; http://www.3gpp.org/specs/WorkItem-info/WI--31008.htm

[7]CC/PP; http://www.w3.org/Mobile/CCPP/

[8]UAProf, http://www.openmobilealliance.org/tech/affiliates/wap/wap-248-uaprof-20011020-a.pdf

[9]http://daml.umbc.edu/ontologies/ittalks/person

visitor is an unknown person, the house owner is asked to register him first before allowing access.

Before sending the mkey to the visitor, the service capabilities of the visitor's phone are checked in order to ensure that an NFC-based key can be distributed. The WURFL code snippet illustrates the service capabilities of the Nokia 6131 NFC mobile phone:

```
<?xml version="1.0" encoding="UTF-8"?>
<wurfl><devices>
<deviceid="nokia_6131nfc_ver1" user_agent="Nokia6131NFC"
 fall_back="nokia_6131_ver1" actual_device_root="true">
   <group id="product_info">
     <capability name="model_name" value="6131 NFC"/>
     <capability name="has_NFC" value="true"/>
   </group>
   <group id="object_download">
      <capability .... />
   </group>
</device>
</devices></wurfl>
```

Upon receiving the mkey, the visitor touches the door lock with his mobile [10]. The NFC reader in the door compares the mkey with a predefined one for that specific lock, taking into account time, date and encryption key. If the visitor's mkey is valid the NFC lock will send an open command towards the control sensor that is attached to the lock.

C. Semantic policy engine

Policy based service access and aggregation is an emerging field in SOA implementations. SOA provides interoperability, but needs policies for access control to the services. Examples of such policies are SMS/Phone services which are restricted to the user of the mobile phone, while the calendar service is available for people specified in the user's profile. Other services regulated by policies might be the collection of sensor data, and health care information for relatives or the health care system. Current solutions based on directory access or standards such as XACML and WS-Policy are not flexible enough and cumbersome to manage. Thus research suggests to move to semantic based dynamic policies[10] without changing the core service logic. Several authors suggest using OWL DL in conjunction with SWRL[11]. The approach is to use the semantic web technologies for user privacy by relation based content access management. Our approach is to extend this idea towards the infrastructure level policy service that ensure fine grained service access and personalized service aggregation.

Performance is also crucial in mobile context aware services. Performance results by Weithöner et. al. [11] shows that of existing reasoning engines performance is not very promising. Chowdhury performed analysis studies identifying the following main performance hindrances [12]:

1) Loading time of ontology
2) Delay caused by ontology based reasoning
3) Time consumed during rule execution (depend on complexity of the rules).

[10] Semantic Identity management SemID, http://www.semid.org
[11] Semantic Web Rule Language, http://www.w3.org/Submission/SWRL/

The main issues with OWL DL are interoperability and scalability as discussed in [13]. OWL DL reasoning is too complex for many large scale contexts, and the expressiveness SWRL provides comes at a cost of computability and efficiency. Efficiency is very crucial in context aware mobile services. Also SWRL neither support non-monotonicity (which means SWRL rules are not capable of modifying the ontology) nor negation as failure.

To formally represent the policies, we use the service contracting framework developed in [14]. It allows process graph and the formalised policy description. Based on the content access scenario in figure 4, we formalise the process graph in 6 and define the following policies:

Pol 1: Each visitor must provide his age (i.e. task $provide\_visitor\_age$ must execute)

Pol 2: If a visitor is categorized as child (i.e. if task $categorize\_visitor\_as\_child$ is executed) then it can not be the case that the visitor can see all content from community CY (i.e. tasks $watch\_CY\_content$ must not execute)

Pol 3: If a visitor is member of community CY and wants to record content, then he must watch content from that community before the recording (i.e. if task $record\_CY\_content$ is executed, task $watch\_CY\_content$ must have been executed before that).

This framework not only allows us to formalize process graphs, but also to find executions that obey policies like the ones we have above. Due to the limited space, we only give a formalisation of the above policies and refer the reader for details to the process and policy language proposed in [14]:

Pol 1: $\bigtriangledown provide\_visitor\_age$

Pol 2: $\bigtriangledown categorize\_visitor\_as\_child \Rightarrow \neg \bigtriangledown watch\_CY\_content$

Pol 3: $\bigtriangledown record\_CY\_content \Rightarrow (\bigtriangledown watch\_CY\_content \otimes \bigtriangledown record\_CY\_content)$

The formalised policy description for content access is part of the policy engine, which administrates access to content, devices and services.

VI. Conclusions

Semantically enriched mobile and sensor services will form the basis of the next generation service world. However the integration of mobile and sensor services into a semantic service execution environment is hampered by a number of factors, specifically the unreliable radio network, round-trip delays and limited capabilities of the devices. This paper addresses service provisioning in a semantic service execution environment. It uses the concept of a virtual mobile and integrates the sensor and mobile services into a Web based semantic service repository.

This concept enables an I-centric service surrounding, where the user, the device and the services are described through ontologies. Our implementation of key elements shows that the xml schema-based device capability descriptions such as WURFL and user profile descriptions such as GUP need to be ported to ontologies. Reasoning based on OWL DL and

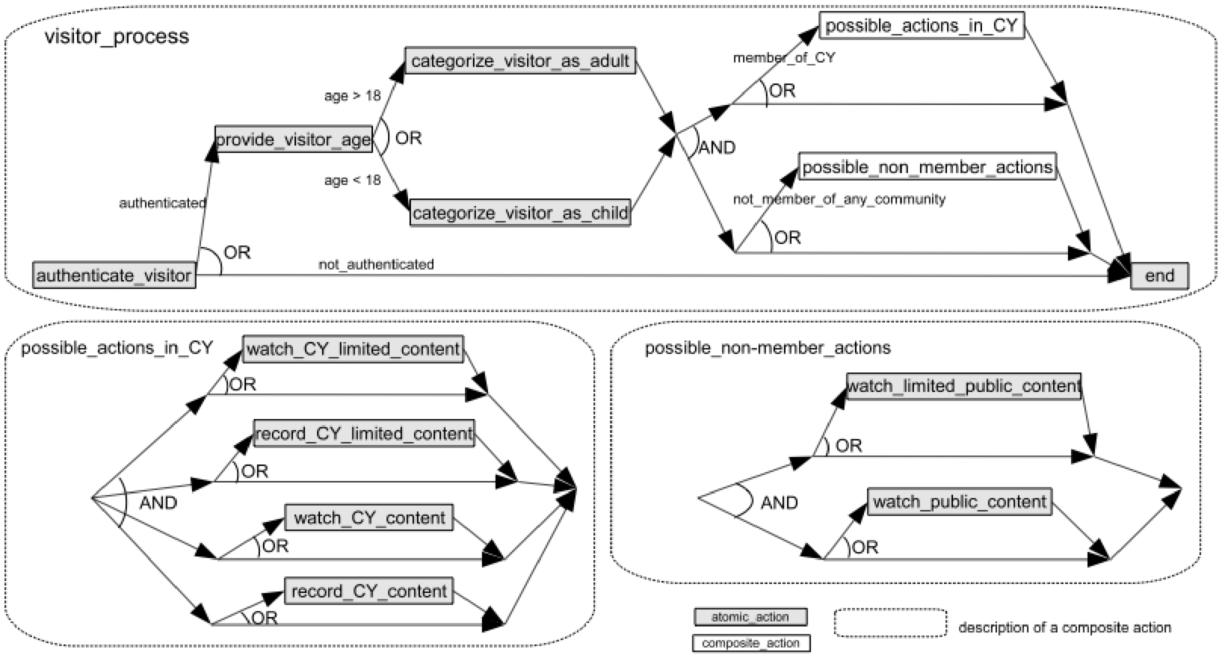

Fig. 6. Formal representation of content access

enhanced by the Semantic Web Rule Language (SWRL) has limitations in terms of expressivity and computing efficiency. It enables however service adaptation based on user profile, service profile and user context. While the current paper demonstrated the use of ontologies for service interaction and policy handling, future work will focus on advanced reasoning capabilities for decision making and implementation of additional elements of our approach.

References

[1] S. Arbanowski, P. Ballon, K. David, O. Droegehorn, H. Eertink, W. Kellerer, H. van Kranenburg, K. Raatikainen, and R. Popescu-Zeletin, "I-centric Communications: Personalization, Ambient Awareness, and Adaptability for Future Mobile Services", IEEE Comm. Magazine, Sep 2004, pp 63-69

[2] M.M.R. Chowdhury, J. Noll, *Identity Management for Wireless Service Access*, in Handbook of Research on Wireless Security, editors Y. Zhang, J. Zheng and M. Ma, Information Science Reference, Hershey, 2008, pp: 104-114

[3] J. Noll, *Mobile Phone Evolution*, Movation White Paper 1/2007, May 2007, http://www.movation.no/index.php?option=com_content&task=view&id=78&Itemid=9

[4] S. Weerawarana, F. Curbera, F. Leymann, T. Storey, D. F. Ferguson, *Web Services Platform Architecture: SOAP, WSDL, WS-Policy, WS-Addressing, WS-BPEL, WS-Reliable Messaging, and More*, Prentice Hall 2005.

[5] T. Gu, Z. Kwok, K. K. Koh, H. K. Pung, *A Mobile Framework Supporting Ontology Processing and Reasoning*, Proc. of the 2nd Workshop on Requirements and Solutions for Pervasive Software Infrastructures (RSPSI '07), in conjunction with the 9th International Conference on Ubiquitous Computing (Ubicomp '07), Austria, September 2007.

[6] P. Rysavy, *Data Capabilities: GPRS to HSDPA and Beyond*, Rysavy Research 2005; http://www.rysavy.com/Articles/rysavy_data_paper.pdf

[7] S. Alam, J. Noll, M.M.R. Chowdhury, *Extending Service Oriented Architectures for Mobile Environments*, Proc. of WWRF #20, April 2008, Ottawa, Canada.

[8] E. Vanem, D. V. Tran, P. Løkstad, T. E. Jønvik, D. V. Thanh, *Virtual Terminal as XML Web Service*, IEEE Trans. Database and Expert Systems Applications, Sept. 2003, pp. 225 - 229

[9] J. Indulska, R. Robinson, A. Rakotonirainy, K. Henricksen, *Experiences in Using CC/PP in Context-Aware Systems*, Proc. Of 4th Mobile Data Management (MDM) Conference, Australia 2003.

[10] J. Noll, J.C. Lopez Calvet, K. Myksvoll, *Admittance Services through Mobile Phone Short Messages*, Proc. Intern. Conf. on Wireless and Mobile Communications ICWMC06, July 29-31, 2006, Bucharest

[11] T. Weithöner, T. Liebig, M. Luther and S. Bohm, *Whats Wrong with OWL Benchmarks?*. Proc. 2nd Intern. Workshop on Scalable Semantic Web Knowledge Base Systems, SSWS 2006, Athens, Georgia, November 2006

[12] M. M. R. Chowdhury, J. Noll, *Semantics Supported Access Authorization Based on Decentralized Architecture*, Intern. J. on Communications of SIWN, 2008

[13] J. de Bruijn, A. Polleres, R. Lara, and D. Fensel, *OWL DL vs. OWL Flight: Conceptual Modeling and Reasoning for the SemanticWeb*. Technical Report DERI-TR-2004-11-10, DERI, November 2004.

[14] D. Roman and M. Kifer, *Reasoning about the Behavior of Semantic Web Services with Concurrent Transaction Logic*, VLDB, 2007, pp 627-638, http://www.vldb.org/conf/2007/papers/research/p627-roman.pdf