METADATA FOR TRUST IN

SERVICE-ORIENTED ARCHITECTURES

Author and co-authors

M. Coetzee[1] and J. H. P. Eloff[2]

Author's affiliation

Information and Computer Security Architectures (ICSA) Research Group

Department of Computer Science, University of Pretoria, Pretoria, South Africa

Author's contact details

[1]marijke@acm.org

[2]eloff@cs.up.ac.za

ABSTRACT

Service-oriented architectures enable heterogeneous applications to be connected together in order to automate a business process. The shift towards this paradigm is largely due to the development of Web Service technologies. For interoperation, trust formation between Web Services is an important requirement. Currently, Web Services do not support differentiated forms of trust, which is required when interacting with either a well-known or unknown party. By inspecting information exposed as metadata, a Web Service can over time, gain a sense of the trustworthiness of other Web Services participating in its environment. In this paper, trust is discussed as it may relate to a service-oriented architecture environment that is implemented with Web Service technology. A novel approach to Web Service trust formation over information is presented. Trust is formed by using information such as metadata that is published through Web Service standards, defined over and above a Web Service interface.

KEY WORDS

Service-oriented architecture, Web Services, metadata, WS-Policy, trust, trust formation

METADATA FOR TRUST IN

SERVICE-ORIENTED ARCHITECTURES

1 INTRODUCTION

Service-oriented computing (SOC) is the computing paradigm that uses services as fundamental elements for developing applications (Georgakopoulos and Papazoglou 2003). A service is a function that is well defined, self-contained, that does not depend on the context or state of other services. Service-oriented architectures are essentially a collection of interacting services that are loosely coupled. In such environments, services are under the control of independent service providers, who may be external or internal to an organisation. In order to eliminate incorrect assumptions about their behaviour, services are required to declaratively define their functional and non–functional requirements and capabilities in an agreed, machine readable format.

Web Services technology (Gottschalk 2002) provides organisations with the ability to exploit this paradigm by enabling location and connection independent Web Services. A Web Service is a type of service, identified by a URI that can be invoked through an Internet connection. Web Services are offered by organisations that support the Web Service implementation, and publish the Web Service description. Requestors interact with Web Services from distant, independent locations, as the necessary information for discovery, selection and binding is made available.

Service-oriented architectures are supported by machine-to-machine interactions that indirectly constitute a quasi form of social collaboration. For such environments, access to resources under the control of one machine, must be granted to large numbers of users who are only known to another machine, in a different domain. The distributed architecture presents some difficulty as user credentials need to be verified across domains. Traditional authentication and authorisation mechanisms cannot rise to meet this challenge. Credential-based access control, where the capability of the user is conveyed in, for example, SOAP headers, provides a viable solution (Hallam-Baker et al 2002), (Coetzee and Eloff 2004). An important requirement is that participants trust each other.

Trust is a positive concept that expresses the belief that the other party will behave as expected, where the belief is based on the lack of contrary evidence (Gambetta 1988). From the current body of research (Marsh 1994), (Grandison 2003), (Dimitrakos 2003), properties of trust have been identified. Properties that are important to mention are: trust is dependent on a specific context or situation; it is a measurable belief that reflects its strength; it evolves with time through new experiences and observations and is subjective.

Considering the nature of Web Services, it is also important to understand how trust is formed between organisations. Trust relationships are influenced by market forces, social interactions, legal and assurance systems and insurance. A model of inter-organisational trust illustrates that trust is established in three stages (Ratnasingam 2001). Firstly, competence trust is established through the trust and security-based mechanisms that are embedded in e-commerce technologies, to provide

speed and real-time accurate information. Secondly, consistent positive behaviours from trading partners lead to credibility and reliability, which creates *predictability trust*. Lastly, *goodwill trust* focuses on organisational reputation and brand names, accomplished by enforcing best business practices.

In society, people learn to trust each other by collecting information through their own experiences, observations, and recommendations from others. For distributed systems, it has been argued that trust should be based on information as far as possible (Jøsang 1996). For Internet applications, trust management has been defined as the act of collecting, codifying, analysing and presenting evidence that relates to competence, honesty, security or dependability, to be able to form trust relationships with others (Grandison 2003).

The main contribution of this paper leads from these statements: to show how information can be used to create trust between Web Services in service-oriented architectures. The approach is uniquely inspired by Web Service metadata that inhabits the XML-based environment. Information is made exploitable for trust reasoning by categorising it. The approach gives a Web Service the ability to determine the trustworthiness of others, at execution time, instead of determining it manually over an extended period.

This paper is structured as follows: section 2 gives a background to the problem. Section 3 identifies information sources that can be used to form trust. Categories are identified that information can belong to in order to enable trust reasoning. Section 4 describes how information can be sourced from the underlying XML-based environment with machine-to-machine interactions to populate information categories. Section 5 concludes the paper.

2 BACKGROUND

Trust between Web service requestors and providers will form the basis of all exchanges that may take place between them. It would be impractical to expect of a Web Service to have the same level of trust and give the same level of access to well known and to unacquainted parties. In order to address trust for Web Services, the Web Services Trust Language or WS-Trust (Della-Libera et al 2003) has been published. It allows interoperability between a Web Service requestor and provider that do not know each other, by enabling them to determine whether they can trust each others' asserted credentials. WS-Trust poses limitations to the establishment trust relationships as it does not enable a Web Service to treat partners and strangers differently. Trust established between Web Services is of binary format, it either exists or it does not.

Current trust management solutions (Blaze et al 1999), (Lampson and Rivest 1996) are focused on solving the problem of distributed access control, and do not reflect the maturity of trust relationships. They present a number of shortcomings to Web Services participating in service-oriented architecture environments. For instance, trusted third parties that are very often required may be absent or inaccessible for some participants; trust is strongly based on cryptographic controls, and is generally defined over the identity of partners; and trust management models are very complex and time-consuming to implement.

To address these shortcomings, an autonomous approach to trust formation is required, where each Web Service makes independent trust decisions based on its own observations. In environments where participants do not know one another, or when participants are far removed from one another, the acceptance of information as truth leads to the formation of trust. This statement is central to the approach defined here. Trust can thus only exist between parties if they know something about each other. For trust formation between Web Services over information, some relevant questions need to be addressed such as: Where does one find the information that is used to create trust? How is the information used? How is trust between Web Services represented?

The result from this paper is an approach to trust based on information that is sourced and associated evidence that is presented. Evidence may for instance consist of certificates for proof of identity, certificates describing competence, and risk assessments. The next paragraph describes relevant concepts for information sourcing and categorisation in order to make information exploitable for trust reasoning.

3 INFORMATION IN SERVICE-ORIENTED ARCHITECTURES

Information about the properties of Web Services plays a central role in service-oriented architectures. Such information is referred to as metadata. Web Service metadata is accessible, as it is machine readable and platform independent. Specifications that extend WSDL (Web Service Definition Language) (Christensen et al 2001) are seen as a prerequisite for service-oriented architectures, as more complex environments have a greater need for Web Service metadata. WSDL defines the characteristics of the interactions between the Web Service requestor and provider. WSDL metadata includes data types and structures of messages, message exchange patterns, and network addresses of endpoints. Specifications to extend features of a Web Service address security, reliability or transactions. These extended features are defined by policy information that is referenced as a set of declarations that state the requirements of the Web Service provider in order to achieve interoperability.

There exists a variety of specifications that enable the definition of Web Service metadata over and above WSDL. WS-Policy (Box et al 2003) can be used over and above WSDL to inform requestors of the non-functional aspects of a Web Service. Even though Web Service requestors may not necessarily be Web Service providers themselves, they can also use WS-Policy to communicate requirements to Web Service providers (Remy and Rosenberg 2004). Quality-of-service issues such as security, privacy, performance and availability that are required and supported, by the Web Service provider or requestor, for SOAP messages to be exchanged, are defined. WS-Addressing (Box et al 2004) defines Web Service endpoint references and associated message properties. To dynamically access any XML, WSDL and WS-Policy metadata, WS-MetadataExchange (Ballinger et al 2004) can be used to retrieve metadata from an Internet address. The establishment of trust that is formed over Web Service metadata and associated information and evidence is thus a reachable goal.

The establishment of trust over information can be observed in human societies. Trust between people is formed by the sourcing of references, experiences, recommendations, and other relevant information. The level of trust that one person holds towards another increases or decreases depending on new information and experiences that is gathered. Humans form trust relationships with others after sourcing and categorising information. Categories allow trust reasoning over

information that is dependent on the personal disposition of each person. In order to portray humanistic trust formation between Web Services, information sources and information categories for trust reasoning are determined in the next two paragraphs.

3.1 Sources of information for Web Services

Common sources of information used to form trust are references, recommendations, experience and environmental information. Each of these sources is defined in the context of Web Services as follows:

- *References:* A primary concern for a Web Service is a lack of knowledge about a new partner. A new partner first needs to prove its competence in a specific domain. If a new partner is endorsed by trusted authorities through references, it can be assigned a basic level of trust. References are statements in the form of certificates from independent third parties.
- *Recommendations:* As it is not possible for a partner to evaluate all aspects of a given situation when making a trust decision, a Web Service can also rely on recommendations from others to form a trust relationship. A recommendation is an opinion obtained from another party, for a specific situation or context such as the delivery of goods or the quality of information provided. It is important to consider how much the third party can be trusted, and what trust can be extended to the party under consideration.
- *Experience:* Trust is also created through the progressive gain of experience with others. Experience refers to the cumulative view of the result of interactions with a party in a context.
- *Environmental information:* For Web Service interoperation, a considerable amount of information has to be made available in a machine-readable format in different XML-based policies. Both the Web Service provider and requestor can describe what they offer and demand from the other party. For instance, information that describes supported security mechanisms of a partner may be useful when trust relationships are formed.

3.2 Categories of information for trust reasoning

When trust is formed between Web Service requestors and Web Service providers, it is influenced by the environment in which interactions occur. In every situation, there may be different types of trust present that will influence the cumulative trust that one party holds towards another. To accommodate this, information is categorised into three distinct classes to allow trust reasoning. Past research defines an ontology that can be used to make these classes explicit (Coetzee and Eloff 2005).

Firstly, *structural* information is based on the properties of the system or institution within which the trust relation exists. Secondly, a Web Service may trust others because of the *belief* that it has in the other party. Finally, a Web Service may have *domain* information that reflects its own expertise. Each of the three categories of information that can be used to reason over trust will now be described in more detail:

3.2.1 Structural information

Structural assurances is information that can be used to give a Web Service the confidence that measures exist that can provide safeguards and reduce the risk when something goes wrong. Legal contracts, assurances and implemented security mechanisms may play a role in trust formation.

- Legal contracts - parties who have a contract with each other have indirect trust in each other, because the judicial system exists and will enforce the contract.
- Assurances - licenses and insurance policies provide additional safeguards to protect against risk.
- Security mechanisms - properties that can most affect a trust relationship are the identity of the Web Services, and the security properties that Web Services offer. Security based mechanisms such as authentication, integrity, and confidentiality ensures timely, accurate and complete transmission and receipt of transactions. In addition, policies, procedures, and standards, encapsulated by best practise ensure smooth functioning of interactions.

3.2.2 Belief information

Beliefs in the other party are information that will determine the extent to which a Web Service can trust others. A comprehensive study of over sixty papers covering a wide range of disciplines, has shown that beliefs can be categorised by honesty, competence, predictability and benevolence (Chervany and MgKnight 1996).

- Honesty is the belief that agreements with a partner are made in good faith. It can be established through recommendations from trusted parties and experiences.
- Competence is the belief that a partner has the necessary skills to do a task. Information that can give a partner confidence in another is certificates from third parties such as ISO 9000 certificates, licenses, credit ratings, audit information and endorsements.
- Predictability is the belief that the actions of a partner are consistent so that a forecast can be made about what such a partner will do in a given situation. This can be achieved by inspecting SOAP messages that are sent and received and by recording for instance: the number of messages in error, the value of transactions, the number of transactions, and the validity of message details.
- Benevolence is the belief that a partner cares about the welfare of the other. It may be established over time as a partner realises the benefits gained from increased cooperation with another party.

3.2.3 Domain information

Domain information is expertise that exists within the environment of a Web Service that can be used to form trust relationships. For example, risk assessments indicate the exposure of a Web Service provider to vulnerabilities and this can affects the trust extended to partners in a given situation. This information does not have to be sourced externally.

The information that is required for each of these categories can be sourced either manually through administrator intervention or automatically by a machine. For instance, information sourced by a researcher on the financial position of a partner may be added to the pool of information by an administrator, whereas information stored in a digital certificate may be processed automatically by a machine. It is also possible that a combination can be used. The next paragraph shows that it is possible for the machines supporting Web Services to source a substantial portion of information for information categories.

4 INFORMATION SOURCING

In order to source and process information, a trust engine is proposed. The trust engine is placed before the Web Service. It is knowledgeable about the requirements of the Web Service, and the standards that are used by the Web Service and its requestors. The trust engine sources metadata, or is presented with various types of information by a Web Service requestor. When a request is sent to the Web Service, the trust engine will intercept it, and refer to independent third parties to verify presented credentials and references. Mechanisms must exist at a Web Service provider and requestor to support the publication of policies, the interchange of references and recommendations, and recording of experiences. Protocols ensure that messages are sent correctly, so that they are understood by communicating parties.

The following interactions define the automated sourcing of information for information categories. Steps 3 to 7 have been shown in figure 1 below:

1. The requestor selects a Web Service. It sends a request to locate the metadata of the provider. A very recent specification, WS-MetaDataExchange defines request-response interactions for this purpose.
2. The provider responds with a set of URIs (Universal Resource Identifiers) that are metadata identifiers.

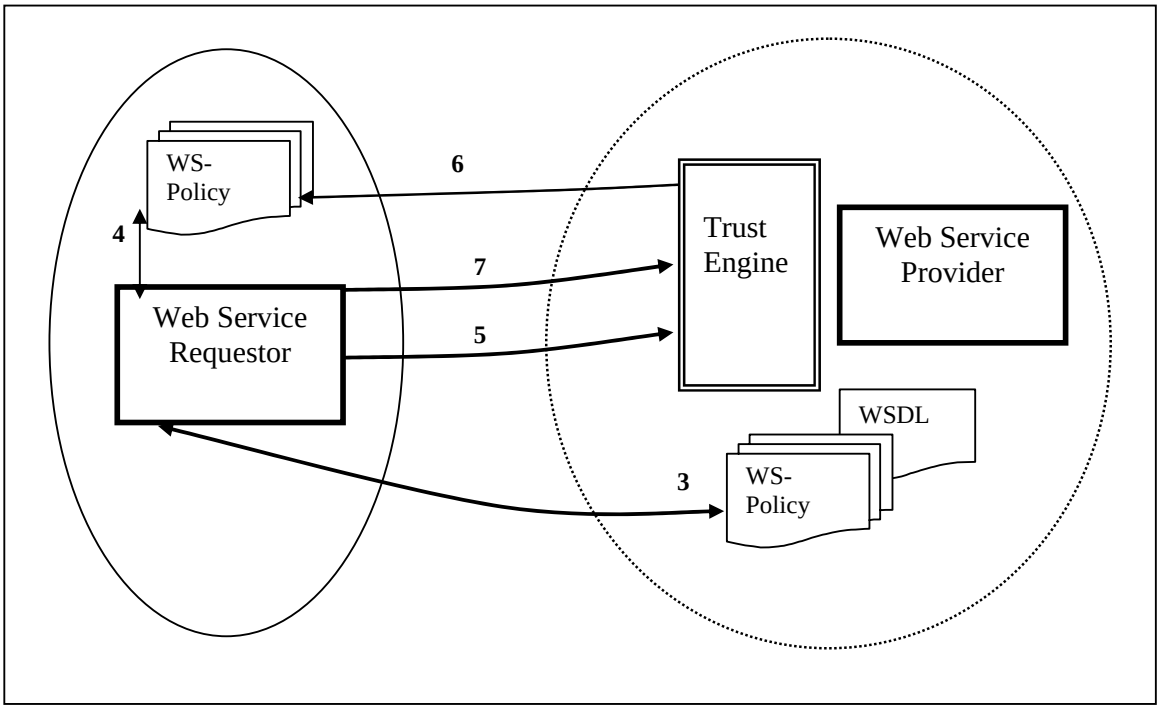

Figure 1: Sourcing of metadata and related information

3. The requestor now retrieves metadata such as the WS-Policy and WSDL documents of the provider to determine its functional and non-functional requirements.

4. The requestor evaluates metadata to determine if the Web Service provider complies with its requirements.
5. It optionally registers with the service. The trust engine establishes an initial level of trust with the requestor based on its identity.
6. The provider retrieves the WS-Policy document of the requestor with the WS-MetaDataExchange request-response interactions. The trust engine uses published information such as supported security mechanisms and independent references to change the trust assigned to the requestor.
7. The requestor submits recommendations made by any of the trusted partners that are found via the WS-Policy document of the provider. Trust is adjusted accordingly.

These interactions can be used to collect information as follows: Firstly, *structural information* can be established by inspecting the WS-Policy documents of partners to establish whether they comply with the security and other requirements of the Web Service. References of partners can be used to establish other assurances. *Belief information* can be established by processing references of partners, recommendations that may accompany requests and recording experiences by inspecting SOAP messages. *Domain* information is not considered here, as it is not collected externally. Values can be assigned to each category after the interpretation of information sources related to it. Values may for instance, vary in the interval [0,1]. After these interactions, the trust engine has a sense of the trustworthiness of the Web Service requestor. Trust is a dynamic, ever-changing metric, which is dynamically adjusted with each new bit of information that is acquired.

The next paragraphs show more detail on how WS-Policy can be used to source information such as supported security mechanisms, independent references, and recommendations in order to establish structural and belief information. It is impossible to determine whether a Web Service is not truthful about its properties. Information such as dishonest behaviour can be recorded as a bad experience, and used in further trust formation.

4.1.1 Security mechanisms

WS-Policy currently communicates to others the security mechanisms it supports through a set of security policy assertions defined within the WS-Security specification (Atkinson et al 2002). To enable secure communication with another party, an endpoint needs to know whether the other party supports WS-Security, and which security tokens can be used. For instance, an endpoint may support any combination of UsernameToken, Kerberos ticket, or certificate, but may prefer a certificate. An endpoint must also determine if the other party requires signed messages, and what token type must be used for the digital signatures. This information allows an endpoint to trust another based on supported security mechanisms.

To enable the further establishment of trust, WS-Policy is extended with new structures to enable the establishment of trust based on references and recommendations (Coetzee and Eloff 2005).

4.1.2 References

The existence of references can be revealed to prospective partners in a WS-Policy document. As a business publishes its own references, a partner needs to confirm the validity of the information with the issuing party. It would be important to know the type of reference, location where it can be found, date created, expiry date and issuing authority. A partner must verify each one before it can be used. The WS-Policy document has the following structure:

```
 <wsref:Reference>
    <wsref:Type>……</wsref:Type>
    <wsref:Location>…… some uri…</wsref:Location>
    <wsref:Name>……</wsref:Name>
    <wsref:Issuer>…some uri…<wsref:Issuer>
    <wsref:IssueDate>……</wsref:IssueDate>
</wsref:Reference >
```

4.1.3 Recommendations

A Web Service can publish a list of partners in the WS-Policy document from whom it would accept recommendations. Prospective partners can use this list to get recommendations that will be trusted by the Web Service. The name and location of the trusted partner can be published, as shown below:

```
<wsbp:Partners>
     <wsbp:Name>……</wsbp:Name>
     <wsbp:Location>……</wsbp:Location>
<wsbp:Partners>
```

Recommendations signed by the issuer are returned to the Web Service in the format shown below. It includes the referee name and location, context of the recommendation, value or degree and the date of creation, and date of expiration.

```
<wsrecm:Recommendation>
      <wsrecm:RefereeName>……<wsrecm:RefereeeName>
      <wsrecm:RefereeLocation>……<wsrecm:RefereeeLocation>
      <wsrecm:Context>……<wsrecm:Context>
      <wsrecm:Value>……<wsrecm:Value>
      <wsrecm:DateCreated>……<wsrecm:DateCreated>
      <wsrecm:DateExpire>……<wsrecm:DateExpire>
<wsrecm:Recommendation>
```

These mechanisms illustrate that Web Service providers in service-oriented architectures are able to express different aspects of their functionality and requirements in metadata, at runtime. As WS-Policy is extensible, a variety of requirements may be expressed.

5 CONCLUSION

This paper discusses the formation of trust between Web Services that participate in service-oriented architectures. The approach to trust formation is based on information that is sourced and categorised. Trust evolves gradually and includes trust in the environment and the underlying control and support mechanisms. This implies the use of security services such as digital signatures, encryption mechanisms, authorization mechanisms, and best business practices, described in policies. In addition, experiences with trading partners and recommendations from trusted referees will influence a trust relationship. Decisions about who to trust and believe is then based on the

properties of a Web Service requestor and the security and trust requirements of a Web Service provider, defined in a policy.

The approach defined here identified information sources, and categories of information for trust reasoning. It illustrated how metadata and other required information can be sourced by a trust engine. Future research will focus on trust reasoning over categories of information. The fact that trust is a subjective and vague concept that is difficult to quantify must be taken into account when choosing reasoning over it. Since fuzzy logic allows reasoning with vague information and models the degree to which trust occurs, it may be suited for use in this situation.

6 ACKNOWLEDGEMENT

The financial assistance of the Department of Labour (DoL) towards this research is hereby acknowledged. This material is based upon work supported by the National Research Foundation (NRF) in South Africa under Grant number 2054024 as well as by Telkom and IST through THRIP. Any opinion, findings and conclusions or recommendations expressed in this material are those of the authors and therefore the DoL, NRF, Telkom and IST do not accept any liability thereto.

7 REFERENCES

Anderson A., et al , (2003), XACML 1.0 Specification, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

Atkinson B, et al, (2002), Web Services Security (WS-Security), Version 1.0, http://www.verisign.com/wss/wss.pdf

Ballinger K, Box D, Curbera F, Davanum S, Ferguson D, Graham S, Liu K, (2004), Web Services Metadata Exchange (WS-MetadataExchange) ftp://www6.software.ibm.com/software/developer/library/WS-MetadataExchange.pdf

Bellwood T., Clement L., Von Riegen C., (2003), UDDI, http://uddi.org/pubs/uddi-v3.0.1-20031014.htm

Blaze M., Feigenbaum J., Ioannidis J., and Keromytis A., (1999), The KeyNote Trust-management System, version 2, IETF, RFC 2704

Box D et al, (2003) Web Services Policy Framework (WS-Policy), http://www.ibm.com/developerworks/library/ws-policy/index.html

Box D, Christensen E, Curbera F, Ferguson D, Frey J, Hadley M, (2004), Web Services Addressing (WS-Addressing), http://www.w3.org/Submission/ws-addressing/

Box D., Ehnebuske D., Kakivaya G., Layman A., Mendelsohn N., Nielsen H., (2000) Simple Object Access Protocol (SOAP) 1.1, http://www.w3.org/TR/SOAP/

Chervany N. L. and Mcknight D. H. (1996), *The meanings of trust*. Technical Report 94-04, Carlson School of Management, University of Minnesota

Christensen E., Curbera F., Meredith G. & Weerawarana S., (2001), Web Services Description Language (WSDL) 1.1, http://www.w3.org/TR/wsdl

Coetzee M.and Eloff J. H. P., (2004), Towards Web Services access control, *Computers and Security*, Vol 23, No 7, Elsevier publishers, UK

Coetzee M.and Eloff J. H. P., (2005), Autonomous trust for Web Services, INC 2005 (The 5th International Network Conference), 5 – 7 July 2005, Samos, Greece

Della-Libera G. et al, (2003), Web Services Trust Language (WS-Trust), http://www.ibm.com/developerworks/library/ws-trust/index.html

Dimitrakos T., (2003), A Service-Oriented Trust Management Framework. In *Trust Reputation, and Security: Theories and Practice*, Rino Falcone, Suzanne Barber, Larry Korba and Munindar Singh (Ed), Lecture Notes in Computer Science, Vol. 2631, p. 53-72, Springer-Verlag

Gambetta D, (1988) *Can We Trust Trust?*, chapter 13, pages 213-237. Basil Black-well, Reprinted in electronic edition from Department of Sociology, University of Oxford.

Georgakopoulos D., Papazoglou M.P., (2003), Service-oriented computing, Communications of the ACM, Oct 2003, Vol 46, no 10, pp 25-28

Grandison T. W. A., (2003), *Trust Management for Internet Applications*, PhD Thesis, Imperial College of Science, Technology and Medicine, University of London, Department of Computing

Hallam-Baker P., Hodges J., Maler E., McLaren C., Irving R., (2003), SAML 1.0 Specification,http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

Jasper R. and Uschold M. A ,(1999), Framework for Understanding and Classifying Ontology Applications, in *Proceedings of the IJCAI99 Workshop on Ontologies and Problem-Solving Methods* (KRR5), Stockholm, Sweden

Jøsang A.,(1996), The right type of trust for distributed systems. In *New Security Paradigms Workshop*, ACM

K. Gottschalk, Graham S.,.Kreger H and Snell J., (2002) Introduction to Web services architecture, *IBM Systems Journal*, Volume 41, Number 2

Kosko. B, (1986), Fuzzy Cognitive Maps, *International Journal of Man-Machine Studies***,** Vol 24, pp. 65-75

Marsh, S., (1994), *Formalising Trust as a Computational Concept*, PhD Thesis, University of Stirling, UK

Modi T., WSIL: (2002) Do we need another Web Services Specification?, www.webservicearchitect.com

Ratnasingam P. P., (2001), *Interorganizational trust in Business to business e-commerce*, PhD thesis, Erasmus University Rotterdam

Remy D., Rosenberg J., (2004), *Securing Web Services with WS-Security*, Sams publishing, Indiana, USA

Rivest R. and Lampson B.,(1996), SDSI - A Simple Distributed Security Infrastructure, http://www.ece.rutgers.edu/~parashar/Classes/03-04/ece572/papers/SDSI.pdf