Appendix A

Definitions of Terms

This appendix lists the terms frequently used in this thesis.

**Service Oriented Computing** - Service Oriented Computing (SOC) is the new emerging paradigm for distributed computing and e-business processing that is changing the way software applications are designed, architected, delivered and consumed.

**Service Oriented Architecture** – Service Oriented Architecture (SOA) consists of three kinds of participants: a service provider, a service requester and a service registry. The interactions involve among these participants are publish, find and bind operations.

**Web Service** - A Web service is a software system identified by a URL, whose public interfaces and bindings are defined and described using XML.

**XML** – The XML (eXtensible Markup Language) is a W3C standard markup language. It is mainly used for the implementations of Web service technologies. WSDL, BPEL, SOAP are all derivatives of XML. Therefore the foundation of Web service technology is on XML.

**SOAP** - Simple Object Access Protocol (SOAP) is a standard message structure used for communication among different Web Services. SOAP messages flow from originator to an ultimate receiver through a SOAP message path. It is a W3C standard available in www.w3c.org/TR/soap
**WSDL** - Web Service Description Language (WSDL) is an XML based language for describing functional properties of Web services. It is a W3C standard available in www.w3c.org/TR/wsdl

**UDDI** - Universal Description Discovery and Integration (UDDI) is an XML-based registry for Web services. It is a place where businesses register and search for Web services. It is a W3C standard available in www.w3c.org/uddi/.

**BPEL** - Business Process Execution Language (BPEL) is an XML-based language to specify business processes that orchestrate the operations of several Web services. It is a OASIS standard available in www.docs.oasis-open.org/wsbpel/2.0/.

**Workflow** – A Workflow is a set of co-ordinated tasks. A Workflow Management System (WFMS) is a software that supports the specification, execution and co-ordination of tasks in a workflow.

**DPW** - The process of document production in an office which is based on a request-reaction-response paradigm is known as Document Production Workflow (DPW).

**MPMSD** - A Multi-Part Multi-Signature Document (MPMSD), D<sub>W</sub>, produced in a DPW W, is an n-tuple, n ≥ 1, such that D<sub>W</sub> = (d<sub>1</sub>, d<sub>2</sub>, d<sub>3</sub>, · · · , d<sub>n</sub>). Each part d<sub>i</sub> in turn is defined as a 3-tuple (m<sub>i</sub>, σ<sub>i</sub>, s<sub>i</sub>), where m<sub>i</sub> is the comment of the reviewer s<sub>i</sub>, and σ<sub>i</sub> is the signature of s<sub>i</sub>.

**Security** - Security is the degree of protection against threats, attacks and vulnerability.

**Threats** - The possibility of an attack is known as threat.

**Attacks** - Any action targeting at the violation of security properties is called an attack.

**Digital Signature** – Digital signatures are analogs of handwritten signatures generally generated by using public-key crypto system. A digital message or its digest is encrypted with a secret key known only to the user. It can be decrypted by its conjugate public-key by
other users for verification. Digital signatures address the issues of user authentication, content integrity, non-repudiation and certification.

**TTP** - An inline Trusted Third Party (TTP) is an arbiter which serves as the trusted intermediate agent in between two communicating agents.

**Audit Trail** - An audit trail is a record showing who has accessed a computer system, resources and what operations are performed by the user concerned during a given period of time.

**Execution Trace** – Execution traces form a subset of audit trails. In execution trace only the current executable data are recorded from the time of initiation to the time of completion. The execution traces need to be captured in different levels like coarse-grain level to the fine-grain level and resources accessed during operations.

**Extra-Tree** - A model to organize execution traces of orchestrated Web services in a tree like structure, named Execution Trace Tree, Extra-Tree in short.

**Obligation** – An operation specified in a policy or policySet that should be performed in conjunction with the enforcement of an authorization decision.


**XML Security** – XML security deals with security of XML documents, which are semi-structured and platform-independent. XML security includes XML encryption, XML digital signature, XML XML cannonicalization etc.

**XML Encryption** - The XML encryption enables encryption of an entire XML document or specific parts of an XML document. It is a W3C standard available in [www.w3c.org/TR/xmlenc-core/](http://www.w3c.org/TR/xmlenc-core/)
**XML Signature** - XML signature provides a useful means of expressing a digital signature over XML data. It is a W3C standard available in [www.w3c.org/TR/xmldsig-core/](http://www.w3c.org/TR/xmldsig-core/).

**XACML** - The eXtensible Access Control Markup Language (XACML) is an XML based language which is required to make authorization decisions. The decision may be permit, deny, indeterminate or error. It is a OASIS standard available in [www.oasis-open.org/committees/xacml/repository/](http://www.oasis-open.org/committees/xacml/repository/).

**Secure Socket Layer** - SSL (Secure Socket Layer) is a technology widely used in browsers and Web servers to create a secure channel between two communicating TCP points. A common protective measure is to send messages over a secure connection using SSL.

**Cross Site Scripting (XSS or CSS)** - This is a type of attack where the attacker inserts malicious code in the request and this will be returned to the victim by that application.

**SWOT** - SWOT analysis is a strategic planning method used to evaluate the Strengths, Weaknesses, Opportunities and Threat (SWOT) involved in a particular system.
Appendix B

Symbols and Notation

This appendix lists the symbols frequently used in this thesis.

\[ \|
\]
Concatenation

= Equality

← Assign

→ communicates to

CL Composite list

PL Participatory list

ETT Execution Trace Table

\( WS_{00} \) Root Web service

\( WS_{10} \) Child Web service

\( WS_{11} \) Child Web service

\( WS_{12} \) Child Web service

\( WS_{20} \) Elementary Web service
\( WS_{21} \) Elementary Web service

\( WS_{22} \) Elementary Web service

\( t_i \) Time of initiation

\( t_c \) Time of completion

\( T \) Transaction number

\( U \) User/who called

\( m_A \) An application submitted by the originator A

\( m_B \) Comment given by the reviewer B

\( m_C \) Comment given by the reviewer C

\( m_D \) Comment given by the reviewer D

\( A_i \) \( i^{th} \) Reviewer

\( A_{i+1} \) Next reviewer

\( I_d \) User-id

\( N \) Arbiter

\( m_i \) Comment of the reviewer

\( m_{i+1} \) Comment of the next reviewer

\( d_i \) Document

\( ps_i \) Policy set

\( s_{attr} \) Attributes of Subject

\( r_{attr} \) Attributes of Resource

\( a_{attr} \) Attributes of action
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_{dec}$</td>
<td>Authorization decision</td>
</tr>
<tr>
<td>$a_{req}$</td>
<td>Access request</td>
</tr>
<tr>
<td>xacml$_{req}$</td>
<td>XACML request</td>
</tr>
<tr>
<td>PAP</td>
<td>Policy Access Point</td>
</tr>
<tr>
<td>PIP</td>
<td>Policy Information Point</td>
</tr>
<tr>
<td>PDP</td>
<td>Policy Decision Point</td>
</tr>
<tr>
<td>PEP</td>
<td>Policy Enforcement Point</td>
</tr>
<tr>
<td>CH</td>
<td>Context Handler</td>
</tr>
<tr>
<td>$S_m$</td>
<td>Storage Manager</td>
</tr>
<tr>
<td>obl</td>
<td>Obligations</td>
</tr>
<tr>
<td>$SK(A)$</td>
<td>Secret key of A</td>
</tr>
<tr>
<td>$PK(A)$</td>
<td>Public key of A</td>
</tr>
<tr>
<td>${}_k$</td>
<td>Encryption/decryption by key</td>
</tr>
<tr>
<td>$K$</td>
<td>Key</td>
</tr>
<tr>
<td>${m}_{SK(A)}$</td>
<td>Digital Signature</td>
</tr>
<tr>
<td>$(m)_{SK(A)}^{PK(A)}$</td>
<td>Verification of digital signature</td>
</tr>
<tr>
<td>$m$</td>
<td>Message</td>
</tr>
<tr>
<td>$\delta_m$</td>
<td>Digest of a message $m$ (encrypted)</td>
</tr>
<tr>
<td>$h()$</td>
<td>One way hash function</td>
</tr>
<tr>
<td>$h(m)$</td>
<td>Hash function of a message</td>
</tr>
<tr>
<td>Symbol</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>$Sk(B)$</td>
<td>Secret key of B</td>
</tr>
<tr>
<td>$Pk(B)$</td>
<td>Public key of B</td>
</tr>
<tr>
<td>$\delta_m$</td>
<td>Digest of a message (decrypted)</td>
</tr>
<tr>
<td>$D_w$</td>
<td>SOAP message/document</td>
</tr>
<tr>
<td>$(d_1, d_2, d_3, \ldots, d_n)$</td>
<td>Previous signed messages</td>
</tr>
<tr>
<td>$s_i$</td>
<td>Reviewer given the comment $m_i$</td>
</tr>
<tr>
<td>$\sigma_i$</td>
<td>Signature of the reviewer</td>
</tr>
</tbody>
</table>
Appendix C

List of Publications

The following list of papers have already been published and accepted:

A. Conference


B. Journal