Lecture Notes in Computer Science

The LNCS series reports state-of-the-art results in computer science research, development, and education, at a high level and in both printed and electronic form. Enjoying tight cooperation with the R&D community, with numerous individuals, as well as with prestigious organizations and societies, LNCS has grown into the most comprehensive computer science research forum available.

The scope of LNCS, including its subseries LNAI and LNBI, spans the whole range of computer science and information technology including interdisciplinary topics in a variety of application fields. The type of material published traditionally includes

- proceedings (published in time for the respective conference)
- post-proceedings (consisting of thoroughly revised final full papers)
- research monographs (which may be based on outstanding PhD work, research projects, technical reports, etc.)

ISBN 3-540-22054-2

Lecture Notes in Computer Science

LNCS LNAI LNBI

Laganá et al. (Eds.)

LNCS 3043

Antonio Laganà et al. (Eds.)

Computational Science and Its Applications – ICCSA 2004

International Conference
Assisi, Italy, May 2004
Proceedings, Part I

Part I

Springer

Lecture Notes in Computer Science 3043

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Antonio Laganà Marina L. Gavrilova
Vipin Kumar Youngsong Mun
C.J. Kenneth Tan Osvaldo Gervasi (Eds.)

Computational Science and Its Applications – ICCSA 2004

International Conference
Assisi, Italy, May 14-17, 2004
Proceedings, Part I

Springer

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Volume Editors

Antonio Laganà
University of Perugia, Department of Chemistry
Via Elce di Sotto, 8, 06123 Perugia, Italy
E-mail: lag@unipg.it

Marina L. Gavrilova
University of Calgary, Department of Computer Science
2500 University Dr. N.W., Calgary, AB, T2N 1N4, Canada
E-mail: marina@cpsc.ucalgary.ca

Vipin Kumar
University of Minnesota, Department of Computer Science and Engineering
4-192 EE/CSci Building, 200 Union Street SE, Minneapolis, MN 55455, USA
E-mail: kumar@cs.umn.edu

Youngsong Mun
SoongSil University, School of Computing, Computer Communication Laboratory
1-1 Sang-do 5 Dong, Dong-jak Ku, Seoul 156-743, Korea
E-mail: mun@computing.soongsil.ac.kr

C.J. Kenneth Tan
Queen's University Belfast, Heuchera Technologies Ltd.
Lanyon North, University Road, Belfast, Northern Ireland, BT7 1NN, UK
E-mail: cjtan@optimanumerics.com

Osvaldo Gervasi
University of Perugia, Department of Mathematics and Computer Science
Via Vanvitelli, 1, 06123 Perugia, Italy
E-mail: ogervasi@computer.org

Library of Congress Control Number: 2004105531

CR Subject Classification (1998): D, F, G, H, I, J, C.2-3

ISSN 0302-9743
ISBN 3-540-22054-2 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 11010043 06/3142 5 4 3 2 1 0

Preface

The natural mission of Computational Science is to tackle all sorts of human problems and to work out *intelligent* automata aimed at alleviating the burden of working out suitable tools for solving complex problems. For this reason Computational Science, though originating from the need to solve the most challenging problems in science and engineering (computational science is the key player in the fight to gain fundamental advances in astronomy, biology, chemistry, environmental science, physics and several other scientific and engineering disciplines) is increasingly turning its attention to all fields of human activity.

In all activities, in fact, intensive computation, information handling, knowledge synthesis, the use of ad-hoc devices, etc. increasingly need to be exploited and coordinated regardless of the location of both the users and the (various and heterogeneous) computing platforms. As a result the key to understanding the explosive growth of this discipline lies in two adjectives that more and more appropriately refer to Computational Science and its applications: interoperable and ubiquitous. Numerous examples of ubiquitous and interoperable tools and applications are given in the present four LNCS volumes containing the contributions delivered at the 2004 International Conference on Computational Science and its Applications (ICCSA 2004) held in Assisi, Italy, May 14–17, 2004.

To emphasize this particular connotation of modern Computational Science the conference was preceded by a tutorial on Grid Computing (May 13–14) concertedly organized with the COST D23 Action (METACHEM: Metalaboratories for Complex Computational Applications in Chemistry) of the European Coordination Initiative COST in Chemistry and the Project *Enabling Platforms for High-Performance Computational Grids Oriented to Scalable Virtual Organization* of the Ministry of Science and Education of Italy.

The volumes consist of 460 peer reviewed papers given as oral contributions at the conference. The conference included 8 presentations from keynote speakers, 15 workshops and 3 technical sessions. Thanks are due to most of the workshop organizers and the Program Committee members, who took care of the unexpected exceptional load of reviewing work (either carrying it out by themselves or distributing it to experts in the various fields).

Special thanks are due to Noelia Faginas Lago for handling all the necessary secretarial work. Thanks are also due to the young collaborators of the High Performance Computing and the Computational Dynamics and Kinetics research groups of the Department of Mathematics and Computer Science and of the Department of Chemistry of the University of Perugia. Thanks are, obviously,

due as well to the sponsors for supporting the conference with their financial and organizational help.

May 2004

Antonio Laganà
on behalf of the co-editors:
Marina L. Gavrilova
Vipin Kumar
Youngsong Mun
C.J. Kenneth Tan
Osvaldo Gervasi

Organization

ICCSA 2004 was organized by the University of Perugia, Italy; the University of Minnesota, Minneapolis (MN), USA and the University of Calgary, Calgary (Canada).

Conference Chairs

Osvaldo Gervasi (University of Perugia, Perugia, Italy), Conference Chair
Marina L. Gavrilova (University of Calgary, Calgary, Canada), Conference Co-chair
Vipin Kumar (University of Minnesota, Minneapolis, USA), Honorary Chair

International Steering Committee

J.A. Rod Blais (University of Calgary, Canada)
Alexander V. Bogdanov (Institute for High Performance Computing and Data Bases, Russia)
Marina L. Gavrilova (University of Calgary, Canada)
Andres Iglesias (University de Cantabria, Spain)
Antonio Laganà (University of Perugia, Italy)
Vipin Kumar (University of Minnesota, USA)
Youngsong Mun (Soongsil University, Korea)
Reneé S. Renner (California State University at Chico, USA)
C.J. Kenneth Tan (Heuchera Technologies, Canada and The Queen's University of Belfast, UK)

Local Organizing Committee

Osvaldo Gervasi (University of Perugia, Italy)
Antonio Laganà (University of Perugia, Italy)
Noelia Faginas Lago (University of Perugia, Italy)
Sergio Tasso (University of Perugia, Italy)
Antonio Riganelli (University of Perugia, Italy)
Stefano Crocchianti (University of Perugia, Italy)
Leonardo Pacifici (University of Perugia, Italy)
Cristian Dittamo (University of Perugia, Italy)
Matteo Lobbiani (University of Perugia, Italy)

Workshop Organizers

Information Systems and Information Technologies (ISIT)

Youngsong Mun (Soongsil University, Korea)

Approaches or Methods of Security Engineering

Haeng Kon Kim (Catholic University of Daegu, Daegu, Korea)
Tai-hoon Kim (Korea Information Security Agency, Korea)

Authentication Technology

Eui-Nam Huh (Seoul Women's University, Korea)
Ki-Young Mun (Seoul Women's University, Korea)
Taemyung Chung (Seoul Women's University, Korea)

Internet Communications Security

José Sierra-Camara (ITC Security Lab., University Carlos III of Madrid, Spain)
Julio Hernandez-Castro (ITC Security Lab., University Carlos III of Madrid, Spain)
Antonio Izquierdo (ITC Security Lab., University Carlos III of Madrid, Spain)

Location Management and Security in Next Generation Mobile Networks

Dong Chun Lee (Howon University, Chonbuk, Korea)
Kuinam J. Kim (Kyonggi University, Seoul, Korea)

Routing and Handoff

Hyunseung Choo (Sungkyunkwan University, Korea)
Frederick T. Sheldon (Sungkyunkwan University, Korea)
Alexey S. Rodionov (Sungkyunkwan University, Korea)

Grid Computing

Peter Kacsuk (MTA SZTAKI, Budapest, Hungary)
Robert Lovas (MTA SZTAKI, Budapest, Hungary)

Resource Management and Scheduling Techniques for Cluster and Grid Computing Systems

Jemal Abawajy (Carleton University, Ottawa, Canada)

Parallel and Distributed Computing

Jiawan Zhang (Tianjin University, Tianjin, China)
Qi Zhai (Tianjin University, Tianjin, China)
Wenxuan Fang (Tianjin University, Tianjin, China)

Molecular Processes Simulations

Antonio Laganà (University of Perugia, Perugia, Italy)

Numerical Models in Biomechanics

Jiri Nedoma (Academy of Sciences of the Czech Republic, Prague, Czech Republic)
Josef Danek (University of West Bohemia, Pilsen, Czech Republic)

Scientific Computing Environments (SCEs) for Imaging in Science

Almerico Murli (University of Naples Federico II and Institute for High Performance Computing and Networking, ICAR, Italian National Research Council, Naples, Italy)
Giuliano Laccetti (University of Naples Federico II, Naples, Italy)

Computer Graphics and Geometric Modeling (TSCG 2004)

Andres Iglesias (University of Cantabria, Santander, Spain)
Deok-Soo Kim (Hanyang University, Seoul, Korea)

Virtual Reality in Scientific Applications and Learning

Osvaldo Gervasi (University of Perugia, Perugia, Italy)

Web-Based Learning

Woochun Jun (Seoul National University of Education, Seoul, Korea)

Matrix Approximations with Applications to Science, Engineering and Computer Science

Nicoletta Del Buono (University of Bari, Bari, Italy)
Tiziano Politi (Politecnico di Bari, Bari, Italy)

Spatial Statistics and Geographic Information Systems: Algorithms and Applications

Stefania Bertazzon (University of Calgary, Calgary, Canada)
Borruso Giuseppe (University of Trieste, Trieste, Italy)

Computational Geometry and Applications (CGA 2004)

Marina L. Gavrilova (University of Calgary, Calgary, Canada)

Program Committee

Jemal Abawajy (Carleton University, Canada)
Kenny Adamson (University of Ulster, UK)
Stefania Bertazzon (University of Calgary, Canada)
Sergei Bespamyatnikh (Duke University, USA)
J.A. Rod Blais (University of Calgary, Canada)
Alexander V. Bogdanov (Institute for High Performance Computing and Data Bases, Russia)
Richard P. Brent(Oxford University, UK)
Martin Buecker (Aachen University, Germany)
Rajkumar Buyya (University of Melbourne, Australia)
Hyunseung Choo (Sungkyunkwan University, Korea)
Toni Cortes (Universidad de Catalunya, Barcelona, Spain)
Danny Crookes (The Queen's University of Belfast, (UK))
Brian J. d'Auriol (University of Texas at El Paso, USA)
Ivan Dimov (Bulgarian Academy of Sciences, Bulgaria)
Matthew F. Dixon (Heuchera Technologies, UK)
Marina L. Gavrilova (University of Calgary, Canada)
Osvaldo Gervasi (University of Perugia, Italy)
James Glimm (SUNY Stony Brook, USA)
Christopher Gold (Hong Kong Polytechnic University, Hong Kong, ROC)
Paul Hovland (Argonne National Laboratory, USA)
Andres Iglesias (University de Cantabria, Spain)
Elisabeth Jessup (University of Colorado, USA)
Chris Johnson (University of Utah, USA)
Peter Kacsuk (Hungarian Academy of Science, Hungary)
Deok-Soo Kim (Hanyang University, Korea)
Vipin Kumar (University of Minnesota, USA)
Antonio Laganà (University of Perugia, Italy)
Michael Mascagni (Florida State University, USA)
Graham Megson (University of Reading, UK)
Youngsong Mun (Soongsil University, Korea)
Jiri Nedoma (Academy of Sciences of the Czech Republic, Czech Republic)
Robert Panoff (Shodor Education Foundation, USA)
Reneé S. Renner (California State University at Chico, USA)
Heather J. Ruskin (Dublin City University, Ireland)
Muhammad Sarfraz (King Fahd University of Petroleum and Minerals, Saudi Arabia)
Edward Seidel (Louisiana State University, (USA) and Albert-Einstein-Institut, Potsdam, Germany)
Vaclav Skala (University of West Bohemia, Czech Republic)
Masha Sosonkina (University of Minnesota, (USA))
David Taniar (Monash University, Australia)
Ruppa K. Thulasiram (University of Manitoba, Canada)
Koichi Wada (University of Tsukuba, Japan)

Stephen Wismath (University of Lethbridge, Canada)
Chee Yap (New York University, USA)
Osman Yaşar (SUNY at Brockport, USA)

Sponsoring Organizations

University of Perugia, Perugia, Italy

University of Calgary, Calgary, Canada

University of Minnesota, Minneapolis, MN, USA

The Queen's University of Belfast, UK

Heuchera Technologies, UK

The project **GRID.IT**: *Enabling Platforms for High-Performance Computational Grids Oriented to Scalable Virtual Organizations*, of the Ministry of Science and Education of Italy

COST – European Cooperation in the Field of Scientific and Technical Research

Table of Contents – Part I

Information Systems and Information Technologies (ISIT) Workshop, Multimedia Session

Information Systems and Information Technologies (ISIT) Workshop, Algorithm Session

Information Systems and Information Technologies (ISIT) Workshop, Security Session

Information Systems and Information Technologies (ISIT) Workshop, Network Session

Information Systems and Information Technologies (ISIT) Workshop, Grid Session

Information Systems and Information Technologies (ISIT) Workshop, Mobile Session

Approaches or Methods of Security Engineering Workshop

Authentication Authorization Accounting (AAA) Workshop

Internet Communication Security Workshop

Location Management and the Security in the Next Generation Mobile Networks Workshop

Routing and Handoff Workshop

A Survey of Web Services Security*

Carlos Gutiérrez[1], Eduardo Fernández-Medina[2], and Mario Piattini[2]

[1] Sistemas Técnicos de Loterías del Estado.
Calle Manuel Tovar 9, 28034, Madrid. (SPAIN). Tel: 34 91 348 92 61
carlos.gutierrez@stl.es
[2] Alarcos Research Group. Universidad de Castilla-La Mancha.
Paseo de la Universidad 4, 13071, Ciudad Real. (SPAIN). Tel: 34 926 29 53 00
{Eduardo.FdezMedina, Mario.Piattini}@uclm.es

Abstract. During the past years significant standardization work in web services technology has been made. As a consequence of these initial efforts, web services foundational stable specifications have already been delivered. Now, it is time for the industry to standardize and address the security issues that have risen from this paradigm. Great activity is being carried out on this subject. This article demonstrates, however, that a lot of work needs to be done in web services security. It explains the new web services security threats and mentions the main initiatives and their respective specifications that try to solve them. Unaddressed security issues for each specification are stated. In addition, current general security concerns are detailed and future researches proposed.

1 Introduction

Recently web services (WS) technology has reached such a level of maturity that it has evolved from being a promising technology to becoming a reality on which IT departments are basing their operations to achieve a direct alignment with the business operations that they support [9]. In fact, based on the most recent reports from Gartner Research, over the next three years, the market for WS solutions will grow steadily reaching $28 billion in 2005 [14]. This seems to be a logical consequence of the numerous advantages offered by the WS paradigm: Standard-based middleware technology; business services high reusability level; easy business legacy systems leverage; and integration between heterogeneous systems.

Due to these immediate benefits, most IT departments are implementing this technology with the high-priority objective of making them operable leaving aside, at least until later stages, the problems related to security. Nevertheless, the industry is still reticent to incorporate this technology due to the low understanding that they have of the security risks involved, and the false belief that they will have to make a costly reinvestment in their security infrastructures. So ensuring the security in WS is crucial to the success of this technology in the industry [11].

WS as distributed, decentralized systems that provide well-defined services to certain (or not) predetermined clients, must be concerned with typical security problems that are common to the communication paradigm, through a compromised channel, between two or more parties. Some of the major inherited security issues that WS technologies must address are authentication, authorization, confidentiality, data integrity, non-repudiation and availability [20].

WS must address both these, inherited from the distributed computing classical scheme, and, in addition, those arising from the new threats created by its own nature. Some of these new threats are:

- Diversity and very high number of standard specifications that do not facilitate a clear vision of the problematic and its solutions.
- The current draft state in which majority of the security specifications are found.
- The Internet publication of a complete and well-documented interface to back-office data and company's business logic.
- Application-level, end-to-end and just-one-context-security communications.
- Ability to federate the full information about the subjects enabling single sign-on environments and boosting interoperability.
- Privacy and anonymity [16].
- Distributed audit.
- Automatic and intelligent contingency processes aimed at being machine-to-machine interactions not controlled by humans.
- A complex dependency network that can lead to the execution of a business process depending on an unknown WS number.
- On-line availability management in critical business processes and management of security policies in large distributed WS environment [10].

The remainder of this article is organized as follows: In section two, a brief review of the core specifications that support the technology at hand is made. In section three, core security WS specifications are explained, and unresolved issues not yet addressed by them are described. In section four, the main initiatives are introduced as well as the specifications related to the security in which they are involved in. In section five, we state some security issues that have not yet been addressed and future research that has to be done.

2 WS Core Standards

In this section, we will take a look at the four fundamental standards involved in the creation of operational WS. Figure 1 outlines the most important security specifications under development. They are grouped as follows:

- Core: WS foundational specifications. These are the standards WS building are based on.
- Core Security: Standards that provides the XML low-level security primitives.
- WS-Security: Family of specification developed by Microsoft and IBM, which are under OASIS standardization process.

* This research is part of the CALIPO project supported by Dirección General de Investigación of the Ministerio de Ciencia y Tecnología (TIC2003-07804-C05-03), and the MESSENGER project, supported by the Consejería de Ciencia y Tecnología of the Junta de Comunidades de Castilla-La Mancha (PCC-03-003-1).

A. Laganà et al. (Eds.): ICCSA 2004, LNCS 3043, pp. 968–977, 2004.

- OASIS: Security specifications developed by OASIS standards body.
- Liberty Alliance Project: Represents the group of specifications developed in the Liberty Alliance Project.

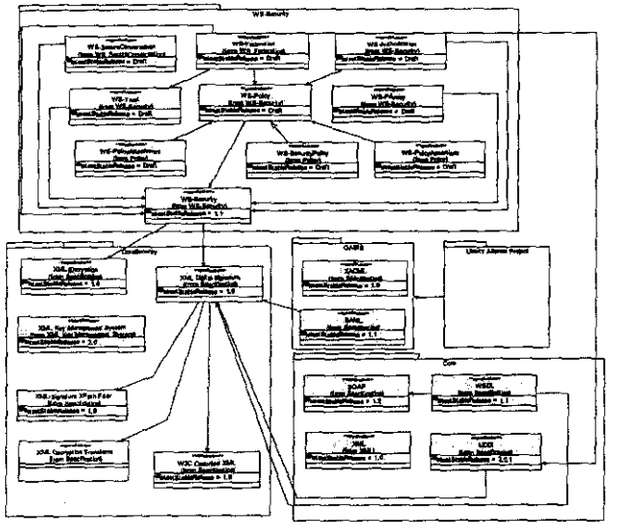

Fig. 1. Current security standards and dependencies, some are optional, among them

Basic services, their descriptions, and basic operations (publication, discovery, selection, and binding) that produce or utilize such descriptions constitute the SOA (Service Oriented Architecture) foundation[18]. WS are built on an architecture SOA basis. In fact, WS architecture is a SOA architecture instantiation [7]. For that reason, the fundamental characteristics described by SOA are the ones that have initially headed the major efforts in the industry standards development process. The core WS specifications are: XML [4], SOAP [19], WSDL [15], and UDDI [3]. These specifications, broadly adopted by the industry, constitute the basic building blocks on which WS are being designed and implemented. The bad news is that they themselves contain security questions that must be answered:

- XML and SOAP: These specifications do not say anything about how to obtain integrity, confidentiality and authenticity of the information that they represent and transport respectively.
- UDDI and WSDL: Should answer questions like: Is the UDDI registry located in a trustworthy location? How can we be sure that the published data have not been maliciously manipulated? Was the data published by the business it is supposed to have been? Can we rely on the business that published the services? Are the services available at any moment? Can we trust the transactions that are produced from the execution of the business services? As we can notice from all these questions, an in-depth analysis of the security problems that an UDDI and WSDL architecture implies has to be carried out [5].

At this point, the main WS standardization initiatives are the World Wide Web Consortium (W3C) and the Organization for the Advancement of Structured Information Standards (OASIS). Both consortiums are trying to standardize their vision, security included, of what the WS should be and should contribute to the WWW world. This parallelism is causing the existence of specifications developed by both groups that resolve similar problems.

All the involved parts will have to make efforts to unify in the future with the purpose of integrating their visions and standards and thus, define a common and global framework.

3 Core WS Security Standards

The W3C consortium is responsible for the development of the following security-related XML technology standards: XML Encryption; XML Digital Signature; and XML Key Management System.

3.1 XML Encryption

W3C XML Encryption [24] provides a model for encryption, decryption and representation of XML document elements. W3C XML Encryption solves the problem of confidentiality of SOAP messages exchanged in WS. It describes the structure and syntaxes of the XML elements, which represent encrypted information and it provides rules for encrypting/decrypting an XML document (or parts of it). The specification states that encrypted fragments of a document should be replaced by XML elements specifically defined in the recommendation. In order to recover the original information, a decryption process is also specified.

Looking back at the beginning of this section, where a list is given of the data-types that can be encrypted, we may miss the possibility of encrypting the tree nodes without having to encrypt full sub-trees. Basically, the solution would consist of extracting the wanted nodes from the original document, encrypt each of them and put them in an encrypted nodes pool. The recipient will get the modified document and the encrypted nodes pool, and it will be able to decrypt the nodes, which it is allowed to see and put them back in place inside the document [12].

One of the implicit security problems associated to this specification is the explicit declaration of the fragments that have been encrypted. According to the specification, information is encrypted and replaced by XML elements containing the result and so, analysis information attacks could be easily be carried out on the output document.

Recursivity is also addressed, but no solution is given. Encrypted key A may need encrypted key B, but B may also need A. The specification states that it is the responsibility of the application that uses encryption to solve these issues.

3.2 XML Digital Signature

W3C XML Digital Signature [1] is a W3C recommendation since 2002, fruit of the joint work between W3C and the IETF. It defines how to digitally sign XML content and how to represent the resulting information according to an XML schema. Digital signatures grant information integrity and non-repudiation. Thus, for example, an entity cannot deny the authorship of a digitally signed bank transfer made through a WS.

According to the XML Digital Signature specification, a digital signature can be applied to any kind of digital content, including XML. Signature creation and verification processes are defined by the specification as well. It is, like W3C XML Encryption, technology independent, so additional mechanisms are needed to define how it will be applied to WS message exchange.

3.3 W3C XML Key Management System

XML Key Management System [21] is a specification that has been subject to the W3C standardization process that proposes an information format as well as the necessary protocols to convert a PKI (Public-Key Infrastructure) in a WS so that it will be able to: Register public/private key pairs; locate public keys; validate keys; revoke keys and recover keys. This way, the entire PKI is extended to the XML environment, thus allowing delegation of trustworthy decisions to specialized systems. XKMS is presented as the solution for the creation of a trustworthy service that offers all PKI subordinate services, but without resolving the inherent issues of the infrastructure:

- How can a Certification Authority's public key be known with total certainty?
- Is the CA ascertained identity useful?
- Known issues with OIDs (Object Identifiers) for automatic processing and their explosive and continuing growth.
- Since the global public key infrastructure is lacking a single world-recognized certification authority, it is not clear how to equip the world in order to allow two systems (ex. WS) that know nothing of each other to establish a trustworthy relationship through a third party on the fly and with no previous off-line communication.

4 WS Security: Standards and Security Issues Already Addressed

Now that we have reviewed the basic WS security standards and their related security, we turn to detail the emerging technology and specifications that are based on these standards. Firstly, we will briefly touch on the WS-* specifications, whose principal developers are IBM and Microsoft. Secondly and thirdly, we will talk about the SAML and XACML standards, which have already been delivered by the OASIS organization in their initial versions, and whose objective is how to present

information and the security policy, respectively. And fourthly, we will briefly comment on the Liberty Alliance project, which is lead by Sun Microsystems.

Table 1. Summary of the current WS standard development efforts grouped by topic.

Authentication	WS-Security, WS-Trust (draft), W3C XKMS (authentication service based on PKI infrastructure, Liberty Alliance Project -> SSO using SAML assertions, WS-Federation -> SSO (draft)
Authorization	OASIS XACML, WS-Authorization (draft)
Confidentiality	W3C XML Encryption, WS-Security
Integrity	W3C XML Digital Signature
Non-repudiation	W3C XML Digital Signature (MAYBE), WS-Security
Security policies	WS-Policy, WS-SecurityPolicy (draft), OASIS XACML
Trust authority	WS-Trust, W3C XKMS
Security contexts/ keys derivation	WS-SecureConversation (draft)
Delegation/Proxy	WS-Trust (draft), Delegation has not been fully addressed yet.
Privacy	WS-Privacy(draft)
Attribute mapping	Not standard-based solution is given yet
Delegation management	Not standard-based solution is given yet
Reference security architecture	Not standard-based solution is given yet
WS Security methodology	Not tandard-based solution is given yet

4.1 WS-Security Family Specifications

IBM and Microsoft, together with other major companies, have defined a WS security model that guarantees end-to-end communication security.These companies are jointly elaborating a series of specifications that compose an architecture, termed by Microsoft as Global XML WS Architecture [8], that will lead the development in the WS industry so that different products can inter-operate within a secured context.

These companies are the original authors of the WS-Security security specification. IBM, Microsoft, and VeriSign developed and submitted it to OASIS, which is responsible of its standardization process. This is the specification on which some additional specifications (some with publicized versions) that cover all aspects of security in WS have based their definition. WS-Security is placed at the base of the security specification stack. Its purpose is to provide Quality of Protection to the integration, adding the following properties to communication and messages: message integrity, confidentiality and simple authentication of a message.WS-Security extends the SOAP messaging framework by defining headers (SOAP Module) to include digital signatures (based on the W3C XML Digital Signature specification) and encrypted data (based on the W3C XML Encryption specification). In addition, it defines and explains the usage of UsernameToken or BinarySecurityToken elements, defined by the specification, which allow the transport of credentials for the authentication of the communication parts.By offering these properties, WS-Security allows the easy incorporation of many existing security models such as PKI and Kerberos.

Other specifications that directly relate to security issues such as WS-Trust, WS-Policy specifications family, WS-Privacy, WS-SecureConversation, WS-Authorization, and WS-Federation are being developed based on WS-Security but they are still in draft form.

4.2 OASIS SAML

OASIS Secure Assertion Mark-up Language [23] is an "OASIS Open Standard" specification developed by OASIS and was delivered in its first version by 2002.

This specification is basically divided in two parts: XML schema definition that allows trust assertions (authentication, authorization o attribute) representation in XML and a client/server protocol to perform XML authentication, authorization and attribute assertion requests. SAML has not yet resolved all the problems related to interoperable XML security-data transferences [13]. However it shows a significant progress. For instance, SAML does not solve how the authentication evidence itself is transferred. This issue has been addressed by WS-Security through its UsernameToken and BinarySecurityToken security tokens definition.

In addition, SAML does not define the way to include SAML assertions within SOAP "wsse:Security" block headers (defined by WS-Security specification). In August 2002, WS-Security specification delivered the technical paper [22] in order to solve this matter.

4.3 XACML

OASIS eXtensible Access Control Markup Language [17] is another OASIS specification since February 2003 and its main intention is to define an XML vocabulary for specifying the rules from which access control decisions can be enforced. XACML is very similar, as far as the security problem it solves, with the policy rules model and language defined by the previously mentioned WS-Policy family specifications. This coincidence is another example of the unification effort proof that an attempt will have to be made in the future to define a sole model and language policy-related in the WS world.

4.4 Liberty Alliance Project

The Liberty Alliance Project [6], led by Sun Microsystems, and its purpose is to define a standard federation framework that allows services like Single Sign-On.

Thus, the intention is to define an authentication distributed system that allows intuitive and seamless business interactions. As we can see, this purpose is the same as WS-Federation specification and Passport's .NET technology ones. Once again, this is another example of the previously so-called overlap problem in WS security solutions.

5 Issues to Be Solved

In spite of the amount of specifications that we have reviewed in this article, and summarized in Table 1, there are a lot of unresolved security issues that will have to be addressed and standardized in the future:

1. A clear effort should exist from all entities involved in this technology in order to unify their criteria and solutions. The explosion of specifications and concepts is such that the learning curve may become unacceptable for the most of the IT projects. As it has been demonstrated during this article, questions like knowing whether the chosen solution is the best of all the possible ones or, if a solution has been chosen, it will be long-term supported by the major industry companies, are difficult to answer.
2. Another problem to be solved is attribute or role principal mapping among different systems. Coherent access control decisions will be difficult to be made when the same name of attributes or roles in both interacting WS are set. For instance, certain set of attributes assigned to user A in system Y may have a completely different meaning in other system B. System B should need to map the attributes provided by user A to its own attributes types in order to be able to make a coherent access decision. RBAC [2] together with a global attribute mapping agreement maybe the way to reach a successful solution.
3. Nowadays, a methodology that accomplishes and consider all the possible security issues and defines an organized development process that directs WS deployments in all expected (and unexpected) scenarios does not exist. This methodology should produce a distributed security framework. This framework would address all the necessary security primitives (authentication, security policy statements, confidentiality ...) and should be flexible enough as to allow primitive implementation solutions replacements without affecting the overall performance of the system. Thus, it should be able to define a framework where specialized security modules maybe plugged in. For instance, it should allow us to replace a WS-Trust security module for a XKMS module in a transparently way for the client. As a first approach we would design this framework by means of a security specialized microkernel creation in such a way. This microkernel would have a central component with not specific functionality beyond that as acting as socket where security modules can be plugged in. Every security module would plug in the socket by means of a well-known interface and would notice to the component about the security primitives it provides. Any client security request will be intercepted by the central component and then redirected to the correspondence security service. The response will be brokered by the central component as well.
4. End-to-end and large scale security policy management. Although several major ongoing efforts on the security policy subject exist (WS-Policy, WS-SecurityPolicy...) they are just specifying ways of representing the policies in XML format while a large scale management solution has not yet been mentioned. This global security policy management framework should propose solutions to issues like dynamic establishment of security policies, end-to-end agreements of many-to-many interactions and security policy version control.
5. The most extended standards and guides for auditing information technologies and managing security [26, 27, 28] do not consider WS yet.
6. Another issue that needs to be addressed is establishing a distributed audit process that allows the reconstruction of situations from data previously recorded. Audit-related data should be stored in some manner during business transactions or when security events (authentication, authorization decisions, etc.) happen. Monitoring this data would allow us to know what is occurring in our system and would permit

us to analyse it when we suspect that a strange situation may have occurred (or in fact has occurred). Due to the distributed nature of WS, where the systems may exist in non-reachable security domains, this audit security data will not always be available for on-line verification. A very desirable feature to design would be one that establishes some sort of special security protocol through which the audit distributed data could be gathered from all possible systems that may have interoperated during certain suspicious business transactions. This way the WS itself may detect the dangerous situation (e.g.: it could compare the current action from a repository of suspicious patterns of behaviour). Then it may obtain all the information about the actions taken by the suspicious subject from all the possible sources, using the audit protocol, in order to build an in-depth detailed trace of his/her behaviour. In addition, this audit protocol would avoid us from having to know the specific storing method used to record the auditable events, thus providing a common way to format, retrieve and convey this information. Therefore, an XML format vocabulary may be defined so that all WS conforming to it would store their audit data in the same way. This audit protocol and XML format may be created as an extension to existing security formats and protocols such as those describe WS-Trust or SAML.

7. Contingency protocols, security alerts management and countermeasures. Similar to the audit protocol mentioned, a contingency protocol could be specified that would allow the propagation, in a standard way, of abnormal security-related events. As a response, countermeasures could be taken automatically by the systems (e.g.: preventing Denial-of-Service attacks).

6 Conclusions

In this article, we have reviewed the current WS security specification and initiatives and we have shown that its diversity is provoking an unclear vision of the problem and their solutions. In addition, unresolved security issues have been stated overall and for each specification. The lack of a global standardization initiative is causing that overlapping solutions to similar problems are being put forward. This fact will require an extra effort in the future not only for the specifications to unify and make themselves interoperable but for industry to adopt and implement them.

Therefore, solutions to topics like security policies, delegation, inter-business principal attributes mapping and privacy are not yet addressed by delivered and final standard specifications.

References

1. W3C XML Signature Syntax and Processing- W3C Recommendation 12 February 2002 (2002). See http://www.w3.org/TR/xmldsig-core/
2. National Institute of Standards and Technology. Role-based Access Control - Draft 4 April 2003 (2003). See http://csrc.nist.gov/rbac/rbac-std-ncits.pdf
3. UDDI Version 3.0.1 - UDDI Spec Technical Committee Specification 14 October 2003 (2003). See http://uddi.org/pubs/uddi-v3.0.1-20031014.htm

4. W3C Extensible Markup Language (XML) 1.1 - W3C Recommendation 04 February 2004 (2004). See http://www.w3.org/TR/xml11
5. Adams, C. and S. Boeyen UDDI and WSDL Extensions for Web Services: a security framework. Proceedings of the *ACM Workshop on XML Security*. Fairfax, VA, USA.(2002)
6. Liberty Alliance Project. Introduction to the Liberty Alliance Identity Architecture (2003). See http://www.projectliberty.org/resources/whitepapers/LAP%20Identity%20Architecture%20Whitepaper%20Final.pdf
7. WSAS. Web Services Architecture Specification - WC3 Working Draft 8 August 2003 (2003). See http://www.w3.org/TR/2003/WD-ws-arch-20030808/
8. Box, D. (2002) Understanding GXA (2002). See http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dngxa/html/gloxmlws500.asp
9. Casati, F., E. Shan, U. Dayal and M.-C. Shan Business-Oriented Management of Web Services. Communications of the ACM, Vol. 46, N° 10, October 2003, pp. 25-28. (2003)
10. Chang, S., Q. Chen and M. Hsu Managing Security Policy in Large Distributed Web Services Environment. Proceedings of the *27th Annual International Computer Software and Applications Conference (COMPSAC'03)*. Dallas, Texas.(2003)
11. Gall, N. and E. Perkins, *The Intersection of Web Services and Security Management: A Service-Oriented Security Architecture*. Computer Associates International, Inc.(2003)
12. Geuer-Pollmann, C. XML Pool Encryption. Proceedings of the *Workshop on XML Security*. Fairfax, VA: ACM Press.(2002)
13. Harman, B., D.J. Flinn, K. Beznosov and S. Kawamoto *Mastering Web Services Security*. Wiley. (2003)
14. RSA Security Inc. Web Services Security (2003). See http://techlibrary.banktech.com/data/detail?id=1065108654_652&type=RES&x=669609469
15. Web Services Description Language (WSDL) 1.1 - W3C Note 15 March 2001 (2001). See http://www.w3.org/TR/wsdl
16. Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V1.1 - OASIS Standard, 2 September 2003 (2003). See http://www.oasis-open.org/committees/download.php/3404/oasis-sstc-saml-sec-consider-1.1.pdf
17. O'Neill, M., P. Hallam-Baker, S.M. Cann, M. Shema, E. Simon, P.A. Watters and A. White *Web Services Security*. McGraw-Hill. (2003)
18. Papazoglou, M.P. and D. Georgakopoulo Service-Oriented Computing. Communications of the ACM, Vol. 46, N° 10, October 2003, pp. 25-28. (2003)
19. W3C SOAP Version 1.2 Part 0: Primer (2003). See http://www.w3.org/TR/2003/REC-soap12-part0-20030624/
20. Sedukhin, I., *End-to-End Security for Web Services and Services Oriented Architectures*. Computer Associates, Inc.(2003)
21. W3C XML Key Management Specification (XKMS) - W3C Note 30 March 2001 (2001). See http://www.w3.org/TR/xkms/
22. WS-Security Profile for XML-based Tokens - Specification 28 August 2002 (2002). See http://www-106.ibm.com/developerworks/webservices/library/ws-sectoken.html
23. SAML. Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1 (2003). See http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf
24. W3C XML Encryption Syntax and Processing - W3C Recommendation 10 December 2002 (2002). See http://www.w3.org/TR/xmlenc-core/