



SWAD-Europe: Deliverable 11.1: Trust Issues Underpinning Scalable Virtual Organisations



Project name:

Semantic Web Advanced Development for Europe (SWAD-Europe)

Project Number:

IST-2001-34732

Workpackage name:

WP 11: Distributed Trust Systems

Workpackage description:



<http://www.w3.org/2001/sw/Europe/plan/workpackages/live/esw-wp-11.html>

Deliverable title:

Framework for Security and Trust Standards

URI:

Authors:

 [Brian Matthews](#), CCLRC.

 [Theo Dimitrakos](#), CCLRC.


 [Juan Bicarregui](#), CCLRC.

Abstract:



Service-oriented computing has emerged as an important new field, distinguished from conventional distributed computing by its focus on large-scale resource sharing including distributed very large data-stores and high-performance networking, and applications such as remote control of experiments and distributed group working in virtual organisations. Given the extreme nature of this computing environment, we consider whether existing leading-edge solutions which focus on the security and trust management of open distributed systems extend to this new paradigm. In this position paper we outline the envisaged architecture and highlight the unique security and trust management challenges which are encountered in such a setting.

Status:

Note: 2004-07-16

Comments on this document should be sent to the public SWAD-Europe mailing list,  public-esw@w3.org,

1. Introduction

The concept of service-oriented computing has been growing over the last five years with the emergence of the Grid [ [Foster & Kesselman 1998](#)], and the Web Service infrastructure [ [Web Services](#)]. This approach seeks to extend the scope of distributed computing to encompass large-scale resource sharing including distributed very large data-stores and high-performance networking, and shared use of computational resources, be they supercomputers or large networks of

workstations.

This concept has been generalised to cover any virtual organisation, defined as any dynamic collection of individuals and institutions which are required to share resources to achieve certain goals [[Foster, Kesselman & Tuecke 2001](#)]. Thus this approach will have applications in commerce and industry, supporting distributed collaborative design and engineering, or supporting distributed supply chains. In these contexts, the emerging Web Services technologies are likely to play a key role, and architecture will be enabling the establishment of trust. Existing approaches to security within distributed systems are stretched by the extreme conditions imposed by the service-oriented approach, and significant effort has been undertaken to provide support for secure use of resources. However, trust thus needs to be established at all levels of the trust hierarchy:

- Authentication: the establishment of identity of the user.
- Policy based management: the provision and deployment of rules and procedures for governing the choice in the behaviour of a managed system towards users who have been successfully authenticated. These include, positive/negative authorisation policies and delegation policies to manage access control; refrain policies to define the actions that subjects refrain from performing on target objects even though they may be authorised to do so; and obligation policies to define the actions that must be performed by managers within the system when certain events occur - therefore responding to changing circumstances.
- Business Rules: the business and legislative framework determining the nature of policies.

In this paper, we discuss the trust requirements imposed by the Service-Oriented Architecture, and propose an approach based on the publication of trust policies and the automatic negotiation of access rights. A similar discussion on requirements is given in [[Foster, Kesselman, Tsudik & Tuecke 1998](#)] which defines the policy which underlies the Globus [[Globus](#)] security model, which uses X.509 certificates as its authentication mechanism. However, that paper does not consider the problems of access control and trust management. It also does not consider how to establish trust between entities which do not have previous knowledge of each other in the absence of a fixed global hierarchy of certification authorities, where the entities may need to discover or dynamically form certification chains in order to enable trust establishment.

2. TRUST REQUIREMENTS ON THE GRID

Consider the following scenario for the use of the Grid.

An engineer within organisation A wants to perform an analysis on a material. By accessing a data portal at site B, she discovers a suitable data set held by a data archive C. The analytical tools are provided at university D within her Virtual Organisation. She initiates the analysis by passing the reference to the data set from B to D, which is then accessed by the analysis tools. D then determines that it does not have enough computational resource available, and determines that a computer is available at different institution E and delegates part of the job there. Finally, D completes the job and return the results to A. D also caches the results of the analysis locally and registers the fact that the precomputed results are available with the portal B and the data provider C. However, the analysis has taken several hours, so the engineer has established a user proxy agent to represent her, collect the results, make payments

as appropriate and close down the collaboration.

This scenario highlights several features of the Service-Oriented Architecture which are relevant to trust.

- Using the Service-Oriented Architecture requires the collaboration of resources which are controlled by different institutions. Each institution will have their own policies on access control and conditions of use.
- The allocation of resource is dynamic; the computational resource at D may not know until part way through the job that additional resource at E is required.
- The user may have different identities in different domains. For example the engineer may have different Users Ids in her own institution, with the data portal, and at the university.
- Resources need to establish trust between themselves (for example, the archive C and the data portal B, the archive C and the analysis tools D, and the tools D and the compute resource E) on a peer-to-peer basis independently of the trust in the original user.
- Resources may be called upon to participate in the task without previous knowledge of the other participants. For example, E may not know the identity of the engineer, or even the institution she comes from. Trust thus needs to be established on the fly so a mechanism needs to negotiate conditions of use, through the delegation of trust from one party to another.
- Different trust conditions may be applied for different parts of the resource, including restrictions on data. For example, the data on the material lodged at archive C may have particular access conditions set by its originators (who may well be elsewhere than at C). A negotiation with respect to the use of the results needs to take place between the archive and the engineer before the data can be sent to the analysis tools.
- Users and resources may delegate their identity to other parties – for example, the user at A creates a user proxy to act her role as the user in the process. The delegation of trust should follow the delegation of identity.
- Users and resources may be located in different countries under different jurisdictions and thus with as a consequence subject to different legal and business requirements.
- Resource usage tracking and charging may be involved. For example, data portal B and computational resource E may be provided as commercial services. They need to identify the correct party to bill and establish trust in credentials (including possibly contacting third parties such as credit agencies) to be satisfied that bills will be honoured. These credentials need to be propagated by other agencies, for example, the analysis tools provider D, who may not be involved in the monetary transaction.

3. TRUST AS INFORMATION

Another more abstract view on the Service Oriented Architecture is that it requires three layers to work effectively [[Jeffery 1999](#)]: firstly a data and computational layer, which provides the raw data sources, processors, and connecting protocols; secondly an information layer over this providing information and location of the underlying resources; and thirdly a knowledge layer to allow reasoning over that information to give intelligent assistance to the users. The traditional Grid infrastructure, such as the Grid Security Infrastructure (GSI) from Globus [[Butler et. al. 2000](#)], has depended on interfaces at the protocol level to provide the security infrastructure. However, this approach has concentrated on authentication and not provided a sufficient infrastructure for the rest of the trust hierarchy exemplified above, especially with respect to authorisation and the

statement and implementation of policies. Further, this mechanism does not appear to have considered the case where the collaborating resources have no prior knowledge of each other (or their certifying authorities).

We propose to supplement this infrastructure by raising the level of the trust analysis into the information and knowledge grids of the layered architecture. This would build upon the established literature in trust analysis, such as [Jøsang 1996] [Dimitrakos 2001] which provides a framework for analysing how trust should be transmitted between agents in distributed systems, especially dealing with how to propagate trust between agents without prior knowledge of each other. The basis of this infrastructure would be the explicit declaration and publication of trust policies by participating resources using a policy specification language, such as Ponder [Damianou et. al. 2001]. Agents wishing to utilise resources would then be able to present their credentials, policies and requirements to the participating resources and an automated process would verify the credentials, possibly referring to trusted third parties, to establish identity, deduce authorisation based upon supplier and consumer policies and to authorise (or not) access under the specified conditions of use. The nature of this task, where statements made of the properties of systems (i.e. policies and requirements from agents) are transmitted across the network, and automatic reasoning is used to determine action from those statements, is in line with proposals under the Semantic Web activity of the World-Wide Web Consortium [Semantic Web]. Consequently, we propose stating the policies and trust statements in using the Resource Description Framework [RDF], and use the emerging tools of the Semantic Web to support the reasoning.

REFERENCES

- [Butler et. al. 2000] *A National-Scale Authentication Infrastructure*. R. Butler, D. Engert, I. Foster, C. Kesselman, S. Tuecke, J. Volmer, V. Welch. IEEE Computer, 33(12):60-66, 2000.
- [Damianou et. al. 2001] *The Ponder Specification Language* N. Damianou, N. Dulay, E. Lupu, M Sloman, Workshop on Policies for Distributed Systems and Networks (Policy2001), HP Labs Bristol, 29-31 Jan 2001.
- [Dimitrakos 2001] *System Models, e-Risks and e-Trust. Towards bridging the gap?* Theo Dimitrakos, Towards the E-Society: E-Business, E-Commerce, and E-Government 1st IFIP Conference on e-Commerce, e- Business, e-Government, Kluwer Academic Publishers, Zurich, Switzerland, October 2001.
- [Foster & Kesselman 1998]. *The Grid: Blueprint for a New Computing Infrastructure*, Edited by Ian Foster and Carl Kesselman, Morgan Kaufmann Publishers, 1998
- [Foster, Kesselman & Tuecke 2001]. *The Anatomy of the Grid: Enabling Scalable Virtual Organizations*. I. Foster, C. Kesselman, S. Tuecke, Intl. J. Supercomputer Applications, 2001.
- [Foster, Kesselman, Tsudik & Tuecke 1998]. *A Security Architecture for Computational Grids*. I. Foster, C. Kesselman, G. Tsudik, S. Tuecke, Proc. 5th ACM Conference on Computer and Communications Security Conference, pg. 83-92, 1998.
- [Globus] *The Globus Project home page* <http://www.globus.org>
- [Jeffery 1999] *Knowledge, Information and Data* Keith Jeffery, CLRC Information Technology Department, September 1999 <http://www.escience.clrc.ac.uk/Publications/9/KnowledgeInformationData.doc>
- [Jøsang 1996] *The right type of trust for distributed systems*. A. Jøsang. In Proceedings of the 1996 New Security Paradigms Workshop, ACM, 1996.
- [RDF] Resource Description Framework (RDF) <http://www.w3.org/RDF/>
- [Semantic Web] *Semantic Web Activity Statement*, World Wide Web

Consortium, 2001 <http://www.w3.org/2001/sw/Activity>
[Web Services] *W3C Web Services Activity* <http://www.w3.org/2002/ws/>