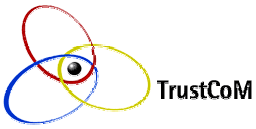

Deliverable

2a

State of the Art Evaluation

WP10 State of the Art – Conclusions and Recommendations

Editor - ICSTM

25/12/2004

Version 1.0

TrustCoM

A trust and Contract Management framework enabling secure collaborative business processing in on-demand created, self-managed, scalable, and highly dynamic Virtual Organisations

SIXTH FRAMEWORK PROGRAMME

PRIORITY IST-2002-2.3.1.9

Prepared for the European Commission under FP6 Contract No. 01945 as a deliverable form

LEGAL NOTICE

The following organisations are members of the Trustcom Consortium:

SchumbergerSema Sociedad Anonima Espanola,
Council of the Central Laboratory of the Research Councils,
BAE Systems,
British Telecommunications PLC,
Universitaet Stuttgart,
SAP AktienGesellschaft Systeme Anwendungen Produkte in der Datenverarbeitung,
Swedish Institute of Computer Scence AB,
Europaeisches Microsoft Innovations Center GMBH,
Eidgenoessische Technische Hoschschule Zuerich,
Imperial College of Science Technology and Medicine,
King's College London,
Universitetet I Oslo,
Stiftelsen for industriell og Teknisk Forskning ved Norges Tekniske Hoegskole,
Universita degli studi di Milano,
The University of Salford,
International Business Machines Belgium SA .

Deliverable datasheet

Project acronym: TrustCoM

Project full title: *A trust and Contract Management framework enabling secure collaborative business processing in on-demand created, self-managed, scalable, and highly dynamic Virtual Organisations*

Action Line:

Activity:

Work Package: 10

Task: State of the Art

Document title: State of the Art: Conclusions and Recommendations

Version: 1.0

Document reference:

Official delivery date: 30/1/2005

Actual publication date: 25/12/2004

File name:

Type of document: Public Report

Nature:

Editors: ICSTM

Reviewers:

Approved by: Michael Wilson

Version	Date		Sections Affected
V.1	25/12/04	All	
V1.1	28/2/05	NRCCL	9 – Legal Aspects

Table of Content

1 Introduction

This document is provided as an addendum to the State of the Art deliverable D2 of the TrustCoM project (IST 01945). It was requested following a formal presentation of the deliverable to the EC and project reviewers, and was given the specific remit of drawing *"clear conclusions from the state-of-the-art studies and recommendations related to the context of the envisioned TrustCoM project plan."* It should therefore be read in conjunction with the aforementioned deliverable as the technologies and conceptual frameworks covered in the State of the Art will be mentioned but not described in this document. Whilst the aim of the State of the Art was to be comprehensive and to identify applicable technologies and conceptual frameworks, this document aims to be analytical and provide a critical viewpoint on the related work. In addition to the remit specified above, we have also attempted to identify particular areas of risk for the project and potential mitigating factors. Most of the existing work related to TrustCoM is comparatively new and still evolving. Wherever possible we have attempted to extrapolate the trend of the current evolution rather than comment on detailed aspects of specific versions. As a consequence of the State of the Art review a number of more in-depth studies were conducted in the last few months as part of Work Package 4 ("Framework Specifications"). These studies aimed to evaluate the applicability of a number of web services (WS-*) specifications to the TrustCoM framework by investigating their use in a prototypical TrustCoM scenario. Although, it is not the aim of this document to give a detailed account of these studies, the conclusions and recommendations presented here take into account their results.

TrustCoM aims to provide an integrated framework enabling secure collaborative business processing in on-demand created, self-managed, scaleable and highly dynamic Virtual Organisations. This objective can be achieved only through the integration of a large spectrum of different tools and techniques that cater for the creation and management of Virtual Organisations, collaborative business processes, contract management and service level agreements, trust management and security. In addition, TrustCoM takes into account the legal aspects of virtual organisations and the socio-economic aspects of business collaboration and in particular fostering trust in business relations and understanding the impact of trust and reputation in the creation and management of virtual organisations. Consequently, this document is subdivided according to the thematic areas of the project in a similar manner to the state of the art deliverable. This also facilitates cross-referencing of information between the two documents.

2 Socio-Economic Aspects

In current business practices, organisations rely heavily on the use of Internet technologies. This has led over the last decade to transformations of the organisational structures and processes that leverage the use of highly dynamic and widespread business collaborations and relations. Two types of business relations are particularly affected by this change: dynamic and possibly transient collaborations for product development, purchasing, sales and services, and dependencies on a wider and more dynamic set of other businesses for the supply of products and services. In this emerging landscape, businesses need strong incentives and mechanisms to trust other businesses. Trust and reputation are concepts that play an increasingly significant role in the formation and maintenance of both business relationships and in the development of market places.

Analyses of the colloquial usages of trust show that it is often overloaded as a synonym for confidence in the ability of an agent (individual or organisation) to undertake a role in a business process (e.g. to have confidence in somebody's ability) within the terms and conditions agreed (e.g. time, quality, cost etc). Reputation is similarly often an evaluation of past performance to perform a role within the terms and conditions agreed in order to determine a measure of confidence in the competence to perform that role in the future. Beyond these usages, studies of trust identify its unique quality as being the intention of a supplier to share the intentions of a customer in circumstances when the agreed terms and conditions (e.g. by contract or SLA) may not apply, or be explicitly broken by the customer (e.g. to supply the goods that were intended, even if they were mis-named in the order; or to supply them to a deadline sooner than that contracted; or to supply the goods to a higher quality level than that contracted). The motivation for the supplier to establish the trust of customers in this specific sense, is to increase the probability of future business. Transfer of reputation and trust across business roles, or contexts have been shown to be important in brand management and the extension of brands to new products. Consequently, trust can transfer to new business opportunities in different ways to competence, and the relation of reputation to trust is more complex than that of reputation to competence. Current computational models of reputation and trust as predictions of risk in fulfilling roles in business processes, and simple legal analyses of contracts or SLAs do not address these unique elements of trust as identified by socio-economic analyses.

It is therefore essential to be able to understand the factors that influence trust related business decisions and the means to foster trustworthiness in a business environment. In particular, the TrustCoM project aims to develop a framework that provides support for trust related information such as risk, trust, experience, evidence and reputation. There are however various ways in which this information originating from the participant members of a VO can be aggregated and transferred across business contexts, in order to identify new partners for the VO or to participate in new VOs. The choice of how to aggregate the various trust information elements has to rely on their perceived value and use in business transactions. To achieve a better understanding of this perceived value and the

behaviour of individuals when faced with trust and reputation information, socio-economic studies have relied on experiments and trust games as well as on empirical observations from consumer systems such as eBay. Experimental studies in the laboratory and empirical or experimental studies in the field are to be considered as important complements.

An established experimental technique for evaluating trustworthiness is the *trust game* introduced by Berg, Dickhaut, and McCabe (1995)[1]. In this game, trust is measured by the amount that one of two players, the *investing player*, unilaterally invests by sending it to the other, the *trusted player*. The trusted player receives three times the amount invested and may then return some amount to the investing player. The amount he returns provides a measure of the trusted player's trustworthiness.

Such trust games and empirical observations have already led to a number of interesting preliminary observations. First, that reputation has monetary value and that trustworthiness can lead to users being prepared to accept higher costs in return for dealing with more trusted partners, second that behaviour differs depending on whether the transactions and participation in the market place are considered short term or long term and third that trust and reputation systems can be maliciously abused for profit. Other more theoretical studies attempt to achieve a better understanding and characterisation of the various components of trust and reputation such as confidence, assurance, good will, commitment and reciprocity.

Conclusions

- An understanding of the factors that underpin trustworthiness in business transactions will influence the TrustCoM framework from two different points of view: first, it will provide the basis for deciding how these factors need to be aggregated in the trust management part of the framework and second, it adds an objective to the overall architecture of the framework which needs to be designed in order to increase trust between the VO partners. Further studies in this direction would therefore be particularly beneficial.
- Equally important is to achieve an understanding of how the other aspects of the proposed TrustCoM framework and in particular the monitoring components, Service Level Agreements and the contract management part of the framework can be used to mitigate the risks, provide increased trustworthiness and compensate for deficiencies in the trust factors e.g., unknown reputation, unknown risk.

Recommendations

- Studies (particularly using the trust game) towards a better understanding of the trust and reputation component factors should be pursued. However, particular attention should be devoted to their combination.
- These studies should also be broadened to address the problem of trust in a wider context comprising assurance mechanisms such as contract management and monitoring.

[1] Berg J., J. Dickhaut, and K. McCabe, 1995, Trust, reciprocity, and social history, *Games and Economic Behavior* 10, 122-142.

3 Frameworks for Virtual Organisations

A large number of studies have already been conducted on the characteristics and behaviour of virtual organisations as well as on enterprise integration reference models. The related work is especially rich in a number of modelling frameworks and notations for expressing the different types of VO as well as their operation. Different types of VO include *targeted VOs* that are characterised by specific goals that the VO attempts to achieve through a deliberate cooperation between the participants as well as *dynamic VOs* that are characterised by the dynamic membership of their participants who may exhibit opportunistic behaviour. A substantial amount of effort has investigated the different operational models of these VO in terms of both their operational business processes and their evolution. A large number of taxonomies have been developed as well as a wide spectrum of techniques for enterprise modelling. Characteristic of this approaches are both the St. Gallen, the CIM/CIMOSA approach, the GIM/GRAI modelling framework as well as the PERA and GERAM reference architectures. However, each of these models, methodologies and reference architectures have distinct focuses e.g. manufacturing processes, human inter-relationships, planning and operations, and whilst all have some valuable input to offer at the conceptual level, none of them has gained widespread acceptance. Also, and more importantly, none provide a concrete implementation that automates the VO management functions and operations or takes into account technology aspects, with the exception perhaps of the RosettaNet implementation framework. The scope of the latter is however strongly focussed on document exchange. Nevertheless, a critical mass of research exists as well as a broad understanding of the issues surrounding enterprise modelling and business-to-business integration.

In contrast to the above approaches, Grid-based models of virtual organisations (e.g., OGSA) focus on practical implementations on lower technology and communication layers for resource sharing and task scheduling and distribution. Although a number of issues relating to service discovery and composition have been addressed as part of these efforts, their focus also constitutes their main shortcoming. Grid-based systems are mostly flat structures where a number of organisations share resources and task execution is distributed but a grid structure is not an autonomous organisation that can itself participate in other Virtual Organisations. Furthermore, although a number of security and access control issues have been addressed, Grid-based systems remain fundamentally open systems where issues of trust (and distrust) between partners focus on usage of resources rather than the confidentiality of information and integrity of systems. Finally, the implementations available form rather monolithic blocks that are not sufficiently modular to offer reuse of independent parts. Owing to the convergence between web service architectures and Grid based architectures, it is expected that the latter implementation issues will eventually be addressed. However, this may not occur in a sufficiently timely fashion to offer TrustCoM a basis for development.

In a similar fashion to Grid-based environments TrustCoM should have an implementation and technology driven approach. The aim is to provide a concrete implementation (or implementation components) that can be instantiated to support the operation of Virtual Organisations even if this implies loss of generality in the VO models that TrustCoM can support. The concrete benefit that TrustCoM can offer to the business landscape is thus not in richer abstractions but in greater support for automation both in the formation and evolution of Virtual Organisations but also in the implementation of their business model through service aggregation. Achieving this will require the development of novel concepts and techniques for:

- providing self-management and adaptability through an integrated policy-based approach
- integrating business processes with service level agreements and the underlying supporting infrastructure
- providing a rigorous yet flexible security model that can adapt to variations of trust between the different partners
- integrating the contract and service level agreement aspects with the trust management infrastructure in order to foster new business relationships
- providing a recursively composable model of virtual organisations

The latter aspect is essential and represents a considerable departure from all existing models. Together with the integration aspects and the policy-driven approach, they constitute the main elements of innovation but also the main challenges that the project faces both at the conceptual level as well as from an implementation viewpoint.

Conclusions

- A number of conceptual models and modelling frameworks have been developed in the course of several collaborative projects that provide valuable input for TrustCoM's conceptual model for VOs. However, particular attention has to be paid to the implementation and technology aspects that are all too often ignored in these studies.
- At the other end of the spectrum Grid-based systems provide some of the core elements necessary for implementing dynamic collaborations. However, they lack a number of conceptual elements required for adequate modelling and automation of VO structures.
- Conceptually, TrustCoM is midway between the former two models and strives to cater for business transactions and recursive compositions of VOs whilst retaining and increasing the level of automation in the VO support infrastructure.

Recommendations

- TrustCoM should develop its own conceptual model for VOs and this development needs to happen as early as possible in the development life-cycle. To this end it is necessary to establish small and highly cohesive teams working on each of the thematic areas (trust, security and contract management) and their earliest priority

should be to explicitly identify the concepts and information provided by the other thematic areas on which their model relies.

- Once completed the conceptual model should be evaluated against the results of past projects that have focussed on modelling frameworks in order to: i) identify additional functionalities that the model can cater for and ii) identify missing functionalities that are judged critical for the development of the TrustCoM framework.
- The success of the conceptual model and of the TrustCoM framework as a whole critically depends on two elements: providing self-management and adaptation, providing integration between the different thematic areas. Both of these aspects need to be addressed early in the architectural and implementation stages. Whilst the initial scoping of the integration effort will be addressed by characterising explicit dependencies between the thematic areas, providing self-management and adaptation is likely to rely on two core concepts that need to be developed and implemented early: business processes and policy (see also Enabling Technologies Section).

4 Contracts and Service Level Agreements

In essence, there are two types of studies belonging to this overall thematic area: work that aims to provide support for managing legal contracts between organisations and automate part of the process associated with their definition and enforcement (e.g., BCA architecture), and work that originates from the network and systems management community relating to customer-provider relationships and the Quality of Service promise associated with a (web-) service (e.g., WSLA, GRASP SLA framework, HP's Web Service Modelling Framework). In addition to the above, a number of parallel studies such as SLAng and the more recent work at SICS aim achieve a better formal treatment of the SLA concepts and notations in order to provide precise semantics and the means to formally reason about the specifications.

The BCA architecture defines a comprehensive infrastructure for dealing with legal contracts comprising sophisticated means of describing contracts as well as processes for contract arbitration and enforcement. However, the framework is rather complex and its implementation status is uncertain. It also does not appear to have been used outside a relatively restricted research environment around the DSTC. From a conceptual view point the framework does however propose a number of solutions that would be worth investigating in conjunction with a legal team.

Work on Service Level Agreements (SLAs) on the other hand is comparatively more mature and better understood. Originally developed as part of the network and systems management community in order to cater for the specification of the Quality of Service (QoS) parameters characterising the provision of network connectivity services, this work has evolved into general frameworks for the characterisation of application level services and more recently business services. Most of the solutions proposed in this area provide the means for: specifying SLAs and associating them with the WSDL services concerned, discovering and locating services based on profiles of QoS that can be delivered for those services, defining simple negotiation protocols for negotiating QoS parameters, and monitoring the compliance with the SLA objectives (including monitoring and metric definition). However, the extent to which these features are supported varies greatly amongst the different SLA solutions proposed. Probably the most concrete framework that is likely to provide a solid foundation for TrustCoM is WSLA, which in addition to specification and structuring of SLA agreements also provides detailed monitoring aspects including an extensible framework for metric definition. The other framework of particular interest is WS-Agreement. Originating initially from the OGSI framework, and a good example of how Grid platforms evolve towards a more open web service environment, WS-Agreement caters for the discovery of services including SLA retrieval and negotiation and is compliant with the other WSRF specifications. WS-Agreement is however a relatively new specification.

ebXML Trading Party Agreement and Collaboration protocol Agreement would also be an alternative. However, their specifications and implementations are tightly

coupled to the other ebXML specifications, which do not seem to integrate well with the other web service specifications.

Conclusions:

- The contract and service level agreement framework in TrustCoM can draw heavily on both the WSLA and WS-Agreement specifications and their implementation support. The aim is to design a framework that caters for both monitoring and enforcement aspects as well as service location and negotiation.
- Support for managing more formal business agreements of the VO needs to also be provided. Although, the BCA provides a significant conceptual model that can help in this development only a subset of the concepts described in the BCA are likely to be required or useful.
- None of the above studies (with the exception perhaps of some later studies on the BCA) examine in detail how trust and reputation information is to be used in conjunction with contracts, SLAs and their associated processes.
- Although, some of the frameworks mentioned above present some features for reacting to SLA violations, this is one of the areas in which TrustCoM could bring a significant contribution.

Recommendations:

- An explicit conceptual model for supporting agreements at both business and service level needs to be developed based on a conjunction of WSLA, WS-Agreement and relevant concepts from the BCA
- The development of this conceptual model needs to devolve significant efforts to two aspects: a) the impact and use of trust and reputation relationships in service discovery, SLA negotiation and enforcement phases and b) the handling of SLA violations in a more flexible form similar to business process descriptions.
- Concurrently, a group formed in conjunction with the legal team in TrustCoM should identify which elements within the BCA and contract management in general are likely to be the most useful within the framework as well as what security controls in terms of confidentiality, integrity and non-repudiation will be necessary.
- Finally, there is a need to identify which specific implementations or parts of implementations could be re-used within TrustCoM.

5 Collaborative Business Processes

By comparison with the other thematic areas considered in the State of the Art, Collaborative Business Processes are probably the best understood and defined technology. Indeed, the issues regarding executable collaborative business processes in the last few years have been more focussed towards standardisation aspects rather than basic research, as many software vendors and business integration consultants are using a wide spectrum of proprietary protocols. Standardisation allows addressing the problems of executable business process aggregation and collaboration across administrative domains that use proprietary solutions as well as outsource workflow control and implementation to third parties. A number of specifications have been investigated including: WS-Coordination that defines the means to coordinate distributed actions during process runtime including agreement on outcome through the propagation of activity contexts, WS-Transactions that extends context information to include transactional capabilities for both atomic transactions (WS-AtomicTransactions) and long running business transactions (WS-BusinessActivity), BPML/WS-CI that focuses on the choreography of message exchanges starting at design time across multiple parties and BPEL4WS that provides the means to describe abstract and executable business processes in terms of their structure, control as well as offered and invoked service interfaces. BPEL4WS and BPML/WS-CI have overlapping functionality, in particular for the business process specification although from different points of view. Whilst BPEL4WS relies on supporting Web Service standards such as the WS-Coordination model, which relies on the use of a single coordinator entity or a hierarchy of coordinators to control the execution of the workflow, WS-CI advocates a more loosely coupled choreography model with distributed control. Since many of the use-case scenarios established for TrustCoM do not explicitly require the use of a coordinator the latter mode may provide some flexibility. Regrettably, development of the BPML/WS-CI has been abandoned with most of the concepts being integrated in a new specification, WS-CDL. The latter however, is still evolving and is not sufficiently stable to base the TrustCoM development upon it, at least during the first stage of the project. WS-CDL is also not catering for a collaborative business process choreography description capturing complex message exchanges across administrative domains, for instance in tendering and quotation processes.

Another option that has been investigated is the use of the ebXML-*series of specifications. However, these do not seem to integrate well with the other WS-* specifications since they advocate their own way of implementing messaging, service repository access, security, etc. It was therefore felt that these should not be investigated further.

Conclusions

- The most promising and stable approach to be used within TrustCoM is based on BPEL4WS/WS-Coordination/WS-Atomic Transaction. WS-CDL should however be monitored for further developments.
- Few, if any of the existing studies address business processes in conjunction with SLAs and none in conjunction with trust and reputation information for service selection and composition.

Recommendations

- Business Process Modelling and implementation should proceed based on the above-mentioned specifications and any available packages providing adequate implementations.
- As the business process infrastructure needs to be deployed for application level services the consortium should investigate further how the same infrastructure can be used to support the administrative and possibly adaptation processes inside the VOs.
- After an initial phase of defining and implementing the core business process functionality, the efforts should focus on two aspects: integration with the SLA infrastructure and leveraging the availability of trust and reputation for providing enhanced flexibility in the enactment of the processes especially across administrative domains.

6 Enabling Technologies

The spectrum of enabling technologies available for TrustCoM broadly divides into the following categories: web service specifications and their infrastructure support, grid technologies, semantic web and ontology based techniques, and tools and platforms for implementation. Implementation tools and platforms further sub-divides in generic platforms and specific tools, implemented before the start of the project by the various partners in the project. Generic platforms have been the focus of more detailed studies as part of Work Package 4 (Framework Specifications) whilst specific implementation toolkits and tools from partners need to be further investigated in Work Package 5 ("Generic Methods and Tools") in terms of actual compatibility and interoperability between the specific implementations.

TrustCoM has made an early commitment to web service standards (WS-*) and associated technologies. This constitutes at the same time an opportunity and a major source of risk for the project. It is an opportunity because in the current state of development, web services seem to be the technology of choice for interoperability and collaboration across heterogeneous implementation domains. It is a major source of risk, because beyond the basic SOAP/XML-RPC communication mechanisms many of the more advanced specifications are still in the draft phase. The specifications are sometimes overlapping and occasionally incompatible as widespread agreement over the set of functionalities that each standard should cover has not been achieved. The implementation status of a number of the specifications is unknown. IBM and Microsoft are the most active players in this arena but their software packages that implement these emerging specifications are frequently updated, incomplete in some respects and the vendors classify the implementations as technology previews.

Of the various standards, SOAP, WSDL, XML Schema, WS-Addressing and WS-ReliableMessaging constitute the basis for communication across domain boundaries. Together they provide the means to describe the functionality of web services, address them in a transport layer agnostic fashion and exchange messages reliably between the various components. In addition WS-Addressing is relied upon by many other specifications. Services need to be discovered and bound to dynamically. Whilst UDDI provides adequate means for registering and discovering services and should be used in the project, it is likely that standard implementations will need to be extended to accommodate the additional information about a service used within TrustCoM such as SLAs associated with a particular service, trust level and reputation.

Event-based asynchronous notifications play a particularly important role within a VO as changes of state need to be communicated to a potentially large and dynamically changing set of components. Two specifications WS-Eventing and WS-Notification would form good candidates for this purpose. Both are robust specifications that define core features for event-based systems, although they lack some state-of-the-art properties. Additionally, the specifications overlap in scope and are currently incompatible because they target slightly different applications.

WS-Eventing is a basic and general-purpose publish-subscribe event-based system. WS-Notification is aimed at management of resources and considered to be used in conjunction with WS-RF. WS-Notification also provides more sophisticated means of managing subscriptions, brokering and topic based dissemination of events. Although, the two specifications are expected to merge at some point in the future, this is not likely to happen during the first phase of development in the project.

To support management of web services and resources using web service-based protocols both WS-Resource (and on tom WS DM MUWS/MOWS) as well as the WS-Management specification (including WS-Transfer and WS-Enumeration) are an emerging effort for getting and setting properties of services. Depending on the requirements of VO management and the maturity of available tools, TrustCoM may use these specifications to perform management operations.

WS-Resource, WS-Management (including WS-Transfer and WS-Enumeration), WSDM or a minimal self-defined service interface will be used for management of web services and associated resources as well as implementing adaptation.

Semantic Web technologies and in particular OWL-S can be used for describing a number of ontological structures related to a VO. In addition to representing structures such as role hierarchies and trust domain OWL-S also permits to publish semantic information related to a web service as well as process models explaining the dependencies between message exchanges. Such models are particularly useful in the cases where mutually intelligible vocabularies of terms for data and process descriptions need to be established between the participants in a VO. However, the expressiveness of OWL-S for web service sharing and integration in a VO context has not been proven yet. In consequence, TrustCoM should focus in a first stage on defining and implementing a working infrastructure for the establishment, evolution and enactment of VOs assuming a single notation for the specifications. Provided this first step is addressed successfully, a generalisation to the use of general ontologies for describing terms and establishing mutually agreed vocabularies can be undertaken in a second phase.

Grid based systems exhibit a degree of similarity with Virtual Organisations and sometimes adopt the same terminology. In particular aspects such as service composition service discovery and simple aspects of SLAs have been implemented and demonstrated. However, Grid-based systems remain open environments focussing on the sharing of resources and distribution of computational tasks. Therefore, they do not address some of the more complex problems related to the recursive composition of VO structures or the use of business processes. Although, a number of security issues have been addressed they also do not cater for recursively-composed structures and do not account for different trust relationships between the participants of a VO structure. From an implementation point of view Grid-environments have been largely monolithic up to now. There are numerous dependencies between the various elements of the frameworks making it difficult to reuse particular tools or components in isolation from the rest. There is substantial expertise within the TrustCoM consortium on building Grid environments and this expertise will be used in the first phase to identify particular tools and techniques that could be re-used within the project.

Conclusions

- SOAP, WSDL, XSD, WS-Addressing and WS-ReliableMessaging should be used as baseline. Extended UDDI should be used for service discovery. WS-Notification and possibly WS-Eventing should be used for Monitoring and Event dissemination.
- WS-Resource, WS-Management (including WS-Transfer and WS-Enumeration) or a minimal self-defined service interface should be used for management of web services and associated resources as well as implementing adaptation
- A number of Grid-services and algorithms could be used, however they need to be extracted from the entire grid-framework and used in isolation.
- Although a number of ontology techniques and in particular OWL-S could be used, these would add an additional level of complexity to the project.

Recommendations

- The project needs to investigate and choose a set of tools and platforms as basis for development. If a particular standard is not supported by existing implementations compliance with that particular standard needs to be abandoned. Attempting to provide interoperable implementations for standards where they do not exist constitutes a major development effort beyond the effort available in the project.
- No more than two platforms need to be selected for implementation. Each platform should have a well-defined set of implementations of the WS-* standards on which it will base any further development.
- Identify if any Grid-based implementation elements can be isolated and reused.
- Use of semantic web technologies and in particular ontologies should be delayed until the basic infrastructure is implemented deployed and tested on a simplified version of the scenarios.

7 Trust Management

Trust management remains a significant area of research despite numerous attempts to address this issue. The fundamental paradox of trust management as a research area is that although there is wide spread agreement on the importance of using trust in a variety of contexts including business transactions and although each one of us has an intuitive belief for what/who we trust, there is little agreement on what trust *is* or how to characterise it. Indeed, the various trust management frameworks proposed in the literature differ significantly both in their definition as well as is their computation of trust. The following aspects are by and large agreed in the various studies on trust:

- Trust is intimately linked (or derived from) different elements such as: recommendation, reputation, risk, and evidence of behaviour.
- Trust is linked to a well identified context that includes the activities being performed, the parties engaged in the interaction as well as other contextual elements of the transactions. However, none of the solutions in existence address this adequately.
- Trust may be expressed in relation to different characteristics of the parties involved in a transaction or the activities being performed such as competence, and honesty of the parties, correctness of the execution of the transaction or its result.
- Trust is quantifiable as otherwise little use could be made of it. However, no consensus has been reached on the desired metrics for its quantification.

The various studies can be broadly divided into two categories, those that focus on trust aspects of a security infrastructure in particular with regards to the authentication of users or disclosure of information and general frameworks for trust management that focus on trust analysis, quantification and trust services. The former are relatively well understood in particular when relating to PKI infrastructures. In addition, there are also a number of emerging studies on trust negotiation i.e., the incremental disclosure of security relevant information such as credentials and requirement for access although further studies are needed in this area. The latter have also been subject of a number of studies but there is little consensus on how to define, manage and compute trust based on an infrastructure of trust services.

Conclusions

- Trust management models need to be developed in TrustCoM together with a supporting infrastructure. Considering the lack of consensus on trust management at the research level it is unlikely that in a VO setting the participants will adopt similar trust metrics or computational models.
- There is some initial work on trust negotiation in terms of incremental disclosure of credentials and requirements. This work can be extended and included in the TrustCoM framework.

- PKI and other security aspects of trust are sufficiently well understood to be used as examples in the over all trust management framework and evaluate a subset of its expressiveness.
- Trust plays a very important role when establishing business partnerships and collaboration and maintaining them over time. However more evidence has to be acquired to demonstrate how trust is incorporated both in the contract content and, foremost, in the operational business processes.

Recommendations

- The trust management infrastructure needs to be agnostic to specific trust metrics or computational models. In addition protocols for negotiation and exchange of trust information need to be developed.
- Security aspects of trust are well understood and should be treated like a specific case in the overall trust management framework rather than as a distinct issue. This will also enable us to test (to a certain extent) the expressiveness and use of the framework.
- Given the current state of the art, it seems reasonable to begin with the development of a trust management model and infrastructure. This should include: what trust services are provided at the VO level and how the information is aggregated from the participants, what specifications of trust metrics and computational models are needed to provide coherent trust information to the decision functions within the VO, how this information will be used as part of SLA management and negotiation, business processes and autonomic security enforcement.

8 Policies and Security

Security aspects of a VO framework span a large number of concerns that broadly divide in the following categories: Access Control, Authentication, Secure Connections, Information Disclosure and Adaptive Security. These will each be addressed in turn in the paragraphs below. Overall security and policy are not only a substantial part of TrustCoM but one where the consortium has considerable expertise.

Access Control Models are well understood within a single administrative domain and new concepts such as Role Based Access Control are increasingly appearing in main stream products. Authorisation policies are used in a number of different frameworks (Ponder, Permis, SPKI, etc) and standards (XACML). Despite apparent differences between the specification languages their functionality is broadly similar. Their enforcement is sometimes different, in particular when applied in distributed environments but the advantages and disadvantages of the various solutions are again well understood. However, distributed access control within environments that cross-domain boundaries remains fundamentally an open research problem. Grid environments have attempted to address these issues in a number of platforms (Akenti, VOMS, CAS, etc.) however the assumptions on which these models are based are too restrictive for VO enforcement. In particular, most grid-platforms are concerned with access control to resources by distributed tasks and do not allow for recursively composable VOs in federated structures (i.e., a Grid is not itself a VO that can participate in higher-level VOs). One common characteristic across all platforms is however the increased usage of arbitrary security tokens to convey relevant security information. As domain boundaries are crossed, local identity loses any meaning and access control decisions are made based on properties that the requestor proves he possesses. These properties may include its role, qualifications and other attributes as well as privileges he/she holds or that have been delegated to him/her. This evolution is also evidenced in the more recent web-service standards such as WS-Trust, SAML and WS-Federation. The latter, in particular, focuses on the exchange and use of such tokens across domain boundaries. WS-Trust and SAML overlap in scope.

Authentication, and in particular authentication based on identity, becomes then a particular case of the more general token based framework described above. Recent studies and standards have particularly focussed on Single Sign-On systems such as Liberty Alliance and Shibboleth. Both of these overlap in scope with WS-Security, WS-Trust, WS-Federation based standards but tend to be less flexible (e.g., lack of support for “active” requestors), focus on identity management alone and rely on SAML for communication of information and SSL as the underlying secure transport protocol.

The WS-* series of specifications provides solutions for message integrity and confidentiality that are specifically tailored the SOAP messages exchanged with web-servicies. These are WS-Security and WS-SecureConversation and have been designed to work in conjunction with the other specifications from the series.

Invariably, access control, authentication and secure connections rely upon the security services being appropriately configured for communication and inter-operation. This is achieved through policies, and thus WS-Policy, WS-SecurityPolicy, WS-PolicyAssertions and WS-PolicyAttachement have been introduced. These specifications aim to provide an interoperable format for policies which can then be embedded and exchanged as secure tokens. Although originally conceived for the local configuration of services the common aspects have been generalised and some advocate the use of these standards for any kind of policies.

The ability to control information dissemination and disclosure including providing restricted access to sub-parts of a document is a long standing research problem. Although expertise exists within the consortium to address these issues, this would entail using a disproportionate amount of effort. In would therefore be appropriate to delay these issues until later on in the project when a security infrastructure is in place.

As often in the past most of the existing work focuses on security mechanisms rather than on the processes required for managing them or adapting their behaviour. Although there are several specifications on how to define policies there is little work on which policies to apply in which circumstances or how policies are dynamically changed in response to changes in context or trust. This issue is of particular relevance in a VO environment characterised by varying trust relationships and where the members and structure of the VO may change. Consequently this is arguably the most important challenge that the TrustCoM security framework will need to address. Even the ability to tackle this challenge is only possible because of the integration with Business Processes, Contracts and Trust.

Conclusions

- WS-Policy, WS-SecurityPolicy, WS-Trust, WS-SecureConversation and WS-Federation form a coherent group of standards that is explicitly focussed on open web-service environments.
- However, several issues need to be addressed in order to combine them in a security infrastructure that satisfies the needs of VO Environments
- Although aimed at being general, WS-Policy and WS-SecurityPolicy remain attached to low level service configuration. Therefore XACML or similar policies may prove more useful ad higher levels of abstraction for use within a VO.
- Information disclosure and dissemination remains a significant issue but it is unlikely that the project will be able to address this, at least in the first phases of development.
- Realising adaptive security represents the most important research challenge. However, little work exists in this area that can be directly leveraged.

Recommendations

- The efforts on security and policy should proceed along two parallel but side-stepped tracks
    1. The definition and implementation of a suitable model for authentication, access control and secure connections within a VO environment
    2. The design and development of the adaptive security model. The starting point for investigation should in particular concern adaptation as a function of trust.
- There is a need to identify early in the projects the implementation available for the WS-* security standards, their degree of maturity and interoperability. The lack of adequate implementation toolkits is a significant risk which would require significant re-development of the model to compensate.
- Attempts to address other issues such as dissemination control should be delayed to the later phases of the project.

9 Legal Aspects

Legal issues play an important part of the TrustCoM framework for three reasons: first because the handling of information such as quantifiable measures of trustworthiness and reputation is information that has legal implications when shared across administrative boundaries, second because the support infrastructure for contracts and service level agreements should provide a legal standing in case of disputes and third because the legal identity and standing of the VO need to be clearly identified when the VO partakes into external contractual relationships either with clients or through participation in other VOs. There is a relatively limited amount of work in the legal domain on these issues; most of it originates from the IST Alive project. This includes a taxonomy of legal issues in VO environments, a reference VO life-cycle from a legal standing, studies regarding legal identity of the VO and studies of the contractual issues as well as definitions for model contracts.

The other area of related work concerns methods for legal analysis. A wide spectrum of techniques have been investigated comprising: conventional legal analysis, legal risk analysis including both conventional risk analysis as well as contract analysis, semi-formal conceptual analysis based on UML representations of the conceptual models and formal analysis, which includes the formalisation of deontic concepts such as obligations, policies, right, power and trust. Conventional legal analysis has an informal form which may be described as a legal argument. It is primarily an activity of the interpretation of norms in relation to given circumstances, typically by a judge deciding a particular legal problem in relation to a case. However, it is questionable if conventional legal methods alone are sufficient for the legal analysis in TrustCoM. Future VOs supported by the TrustCoM framework will be interested in understanding and solving legal problems in advance, rather than deciding a particular legal problem when a dispute occurs. The legal analysis in TrustCoM should therefore seek to combine conventional legal methods with other methods that support a proactive legal risk management.

Conclusions

- The work in the Alive project provides a solid foundation from which to start the analysis. The Alive project has among other results produced model contracts that can assist in addressing some of the typical legal risks related to the different phases of a VO lifecycle. However, this template needs to be adapted to the specific risks that a particular VO may face.
- The VO model contract provided by Alive is envisaged as a high-level text-based contract drafted and monitored by humans. In addition to this contract level, VOs may enter into more specific and operational electronic contracts and SLAs, where contract drafting and/or monitoring may be automated. For the time being, a fully-automated drafting and monitoring of the rather complex high level VO contract as provided in the Alive template does not seem feasible. However, this does not mean

that the TrustCoM framework can ignore the high-level contracts. TrustCoM should provide tools and methods to support the drafting and monitoring of text-based VO contracts. These tools and methods should focus on the management of legal risks related to the participation in a VO.

- The advantage of the TrustCoM legal team is that it comprises substantial expertise for performing traditional legal analysis as well as both semi-formal and formal analysis of VO issues. This will allow a multi-disciplinary research, where legal concepts are not only described in a textual form, but also expressed applying semi-formal and formal methods. These different disciplines need to be integrated in a way that ensures that the analysis results are relevant for the overall project. The most promising integration of these different methods is a model-based legal risk analysis based on both semi-formal and formal methods.

Recommendations

- The legal analysis should be based on the scenarios developed by the TrustCoM prototypes in order to ensure the relevance for the overall project. In particular, the TrustCoM scenarios should be used to uncover typical legal risks and to identify suitable treatments, with a particular focus on trust management, security management and contract management.
- The output that is expected from the legal risk analyses should consist of both textual and semi-formal representations of the identified legal risks with respect to the analysed scenarios as well as suitable treatments, with a particular focus on trust management, security management and contract management.
- The TrustCoM VO framework should support the drafting and monitoring of VO contracts at all levels, regardless whether or not they can be fully formalized. Hence, TrustCoM should also develop mechanisms (tools, methods and languages) for identification, assessment and treatment of legal risks to be dealt with in high-level VO contracts drafted and monitored by humans. These mechanisms should facilitate bridging of the communication barrier between experts within the legal domain and other relevant domains by applying graphical models of legal risks and treatments, which can be understood by professionals from different domains. These mechanisms should be seen as complementary to other TrustCoM methods and tools that primarily focus on the VO contract management level which can be fully formalized and automated.
- The graphical models for legal risk analysis should primarily be based on UML. Formal methods may be used to provide precise semantics for the graphical models.

10 Conclusions

Although a number of points have been presented in each of the thematic areas discussed above, together with conclusions and specific recommendations for each area, the most salient concerns deserve to be re-iterated here.

- **General project approach.** There is a large amount of literature across all thematic areas that has developed a substantial number of models, many of which aim to be exhaustive. Few of these models have been the subject of consensus in the research community, have been validated in any realistic fashion, or have been adopted by industry. Therefore, TrustCoM should strive to simplify its models wherever possible and address concerns from a practical and implementation-oriented point of view rather than purely from a modelling stance. It is worth re-iterating that TrustCoM is an industry-led integration project rather than a pure research endeavour.
- **Web-service standards specifications.** TrustCoM has made an early commitment to web-service standards. Although a reasonably comprehensive package of specifications exist, the availability of implementation toolkits for these standards as well as their maturity and interoperability is less clear. This is a significant risk because the TrustCoM consortium does not have sufficient resources to develop or debug implementations of the standards where they are missing. It is therefore recommended that based on the demonstrator environments a maximum of two implementation profiles be defined. These should comprise implementation toolkits for all of the WS-* standards that TrustCoM aims to use and interoperability between them should be demonstrated. Steps towards establishing this have already started within the project but this effort needs to be concluded when the first version of the architectural models is available.
- **Legal and socio-economic issues.** A major advantage of TrustCoM is the emphasis put on legal and socio-economic issues. As always however, there is a danger that these studies diverge in directions that are relevant but that cannot be supported by the TrustCoM framework. It is therefore important to periodically reassess the focus of these studies in order to maximise the input that they provide to both the conceptual modelling and the software implementation within the project. The studies of socio-economic and legal issues should have a clear focus on the scenarios developed and used in TrustCoM, in order to ensure that they address the business cases to be supported by the TrustCoM framework.