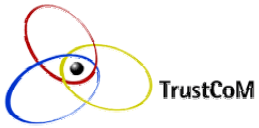


Deliverable

61

TrustCoM Roadmap

Scientific and Technological Assessment of the project & Scientific and Technological Roadmap

WP12 S&T Roadmap

Theo Dimitrakos

Scientific coordinator, TrustCoM project

BT Group, Chief Technology Office

28 August 2006

Version 2

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

Networked business and governments

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:

Atos Origin,
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 Science 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 Kent,
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:	**7**
Activity:	**7.3**
Work Package:	**12**
Task:	**12.4-8**

Document title:	**Progress Assessment and S&T Roadmap**
Version:	**2**
Document reference:	
Official delivery date:	**31 July 2006**
Actual publication date:	
File name:	**TrustCoM.D61.SnT.Roadmap.V2**
Type of document:	Report
Nature:	Restricted

Authors:	Theo Dimitrakos (BT) based on input from Florian Kerschbaum (SAP), Ivan Djordjevic (BT), Christian Geuer-Pollmann (EMIC), Jakka Sairamesh (IBM), Lutz Schubert (HLRS), EmilLupu (IC), Pablo Giambiagi (SICS), Philip Robinson (SAP), Joris Claessens (EMIC), Tobias Mahler (NRCCL), David Golby (BAE Systems), Paul Kearney (BT), David Chadwick (U. Kent), Frederica Paci (U. Milano)
Reviewers:	Jürgen Doser, Burkhart Wolff (ETH) Ignacio Soler (Atos Origin)
Approved by:	

Version	Date	Sections Affected
0.1	May 2004	First version of the S&T Roadmap.
0.2	August 2004	Minor update
0.3	November 2004	Major restructuring – all sections affected
0.4	February 2005	Major restructuring – all sections affected
0.5	April 2005	Minor update
0.6	July 2005	Major update – "self-assessment" and "recommendations" sections affected (sections 7 & 8 in v0.6).
0.7	August 2005	Minor update / aesthetic improvements
0.8	September2005	Undergone internal reviews and QA procedure
0.9	September2005	Minor update
1.0	September2005	Final version delivered
1.1	December 2005	Minor update to reflect project progress
1.2	March 2006	Minor update to reflect project progress
1.3	July 2006	Major restructuring all sections affected
1.4	August 2006	Updated input on assessment and recommendations
1.5	August 2006	Integration of internal reviews on assessment input
2.0	August 2006	Final version for internal review
2.0	September 2006	Final version updated with feedback from the internal review

Table of Content

1 About this document

This document is the main deliverable of the TrustCoM scientific & technological roadmap. Work started at the beginning of the project (month 1) and will last until month 36. Its main objectives are

1. to periodically revisit, update and refine the research challenges faced by the TrustCoM Consortium, taking into consideration the interests of the TrustCoM Consortium, progress within the project, and the advancements achieved outside of TrustCoM
2. to produce a comprehensive scientific and technological roadmap guiding the research advancements and technological innovations expected during the project's implementation towards meeting the identified research challenges
3. to conduct a self-assessment of the project's progress towards meeting its research and technological objectives
4. to offer specific recommendations in order to improve delivery or re-adjust the ongoing technical work towards converging goals and common research objectives

This deliverable does not have the following objectives that are sometimes attributed to general-purpose roadmap documents.

- It does not attempt to analyse the problem space addressed by the project and scope its objectives in relation to that problem space. Although section 3.2 sketches indicative examples of Virtual Organisations of interest for TrustCoM, see [2] for a detailed analysis of the problem space.
- It does not attempt to analyse the state of the art outside of TrustCoM and define how TrustCoM is positioned against the state of the art. Section 4 highlights the most critical advancements to the state of the art for each research that is tackled by TrustCoM. For an analysis and evaluation of the state of the art it draws on [1].
- Section 4 summarises the most relevant standards and design patterns for each area of TrustCoM innovation. However, this deliverable does not attempt to analyse in detail the relevant Open standards in these areas, nor does it offer a roadmap towards integrating or extending these standards. See [**15**] for such an analysis.
- Section 6 indicates the key beneficiaries of the business pilots stemming from the TrustCoM framework and section 4 indicates the beneficiaries of the main by-products in each area of innovation. However this deliverable does not attempt to analyse the exploitation and business opportunities in the areas addressed by TrustCoM or to identify exploitable products within the project and to classify them against identified business opportunities. This is addressed in [4] and [14].

Particular emphasis is placed on achieving the necessary integration that will underpin subsequent scientific advancements and technological innovation. This Roadmap is a "live" document updated as necessary throughout the project and revised at the end of each stage of a project phase.

Some specific questions that are addressed by this deliverable include the following:

- What has changed in the environment since the initiation of the project?
- What is the impact of these changes in the objectives of the overall project?
- What is the recommended reaction of the Consortium to these changes, what can be addressed within the TrustCoM project and what has to be done by other – potentially new – projects?
- For each research challenge initially identified in the technical annex of the project (or earlier versions of this roadmap):
    a. Has the assumption of this challenge changed?
    b. Must it be updated? If so, how?

c. For each change identified: does the change have impact on the project activities targeting this challenge?

d. After the end of the TrustCoM project, can it be foreseen that the project will not solve this challenge, but new challenges have appeared?

1.1 Outline of this deliverable

The rest of the deliverable is structured as follows:

Section 2 offers a general introduction where we describe the process of producing this deliverable is explained and the overall impact of the S&T roadmap on the project.

Section 3 provides an overview of the TrustCoM project, the motivation for this research in general and a summary of the high-level research challenges. In particular, section 3.2 offers examples of Virtual Organisations that are of relevance to TrustCoM and section 3.4 in particular offers an overview of the technical core of the TrustCoM framework. Section 3.5 offers a graphical representation of the projected timescales of the TrustCoM innovation from conception to market penetration.

Section 4 highlights the main innovations of the project and summarises a self-assessment of technical progress and impact. There is a subsection (4.1-5.2) dedicated to each technical core and contextual themes of the integrated project. Each of these subsections starts by reviewing the technical goals and research challenges set for a theme and summarising relevant aspects of the current state of the art and relevant standards. Then it provides a summary of the main research achievements, innovations and technical results of the project in each area. It concludes by identifying areas for further research after the end of the project and, where appropriate, indicates which steps in that direction are planned for the remaining of the project.

Section 6 summarises the selected business pilots, the key stakeholders involved, the anticipated business impact and the main beneficiaries of the TrustCoM framework seen as an integrated product, service platform or infrastructure. Recall that beneficiaries of specific by-product, such as services relating to a single technical area, are already mentioned in Section 4. By leveraging design principles and best practices from the Service-Oriented-Architecture (SOA) paradigm, we have ensured that one could either use the TrustCoM framework as a whole or re-use the designs and prototypes relating to any of the core technical theme without necessarily having to buy into the rest.

Finally, section 7 concludes by revisiting the main recommendations and highlights topics of particular interest after the end of the project.

The bibliography at the end of the project offers references to project deliverables that provide more detail about the products and innovations mentioned in this report.

2 Introduction

The TrustCoM project [http://www.eu-TrustCoM.com/] is developing a framework for trust, security, and contract management for secure, collaborative business processing and resource sharing in dynamically-evolving Virtual Organisations. An overview of the motivation, targeted application domains, and of the scientific and technological objectives of the project is described in section 3 of this report. The term "TrustCoM Framework" stands for the principles and paradigms, the processes and functions, and the architecture and the technology that underpin trustworthy, secure, and contract-driven operations of Virtual Organisations.

The purpose of this document is to provide a coherent overview of the scientific and technological objectives of the TrustCoM project, to highlight main research results, and to update research challenges and associated technical goals, and to provide the foundation for research and technological development work to be completed in the final phase of the project.

2.1 Towards the TrustCoM scientific & technological roadmap

This document is the main deliverable of the TrustCoM workpackage: scientific & technological roadmap. Its main objectives are to set the main research challenges of the project, to produce a comprehensive scientific and technological roadmap guiding the research advancements and technological innovations expected during the project's implementation towards meeting the identified research challenges, and to conduct regular progress assessments in order to re-adjust targets and focus of the work. This report updates [13] and covers an assessment of the project so far, offers recommendations for the remaining of the project and highlights topics for further research and development after the end of the project.

The Roadmap is a "live" document, updated as necessary throughout the project and revised at the end of each stage of a project phase. The process for the development and update of TrustCoM scientific and technological roadmap consisted of the following steps:

1. Validation of the research challenges by the project consortium and the associated communities. This included steering the work conducted in the following tasks:
    a. *Selection of a number of targeted application domains* and analysis of several scenarios in order to identify the main issues relating to the security, trust and contract management across various Virtual Organisation settings. Scenarios in selected areas have been analysed in order to validate the research challenges, on one hand, and to inform the scientific and technological objectives on the other. The analysis was conducted during the first quarter of the project and results of the analysis have been documented in [2]. The scenarios pursued in the remaining of the project amalgamate elements that have been identified as critical by this analysis. Based on the results of the work on testbeds and on exploitation, two groups of scenarios have been selected for final demonstration, these are described in detail in deliverables [16] and [17].
    b. *Analysis and evaluation of the state of the art*. One of the intrinsic characteristics of all projects dealing with ICT infrastructures and technologies for Virtual Organisations is their dependence if a large number of potentially diverse enabling technologies. From early on in the TrustCoM project we tried to make sense of this large technology jigsaw and identify what could be leveraged upon, what had to be improved and what had to be developed from scratch in the context of this project or in collaboration with a wider community. The analysis was conducted mainly in the first quarter of the project and updated at the fifth quarter of the project. The results have been documented in the *State-of-the-art-Evaluation* [1]. This evaluation has been very informative and covered an unprecedented number of the technologies that have not been analysed before by the same team and in a common context.

c. *Identification and analysis of a set of open standards* that can be used as a foundation for the TrustCoM framework or relate to specific aspects of this framework. A standardisation roadmap was produced refined periodically in line with continuing project efforts and developments outside of the project. Standards cover areas from service management to identity management and federation, and from messaging to business processing. The number and complexity of the standards that have been analysed, classified and experimented with, has been unprecedented for a research project, and the knowledge generated has been particularly useful for understanding how ICT for Virtual Organisations can be designed and developed.

The combined outcome of the work lead into a revision and subsequent refinement of the initial project objectives that was in turn channelled into the two main action lines of the project: the first one that focuses on conceptual models and architecture and the second one that focuses on detailed design and reference implementation of key ICT services and components in the areas of security, trust and contract management for dynamic Virtual Organisations.

2. Communication, validation and revision of initial challenges via specific outreach activities. In particular, the TrustCoM project

   a. Ensured that the initial challenges and key results have been extensively discussed and accepted among all Consortium partners and in particular software vendors and end-users.

   b. Presented and discussed our approach, results and exploitable outputs with a business advisory board that includes senior managers and strategists from the lines of business of the key stakeholders within and outside of the TrustCoM Consortium.

   c. Organised a series of detailed tutorials and panel discussions during the 2nd, 3rd and 4th international conferences on Trust Management (iTrust) where the targeted application domains, evaluated technologies and relevant standards were discussed with the community.

   d. Organised a panel discussion for feedback on initial results during a workshop at the 18th IFIP World Computing Congress.

   e. Organised two workshops with extensive presentations of research challenges, plans and results of the evaluation during the eChallenges conference.

   f. Lecture and tutorial on interim findings and project plans at the FOSAD international post-graduate school on Foundations of Security Analysis and Design, September 2005.

3. Clarification of the main aspects that may appear in a “blue print” of the TrustCoM framework. This was achieved by steering the work in Action Line 1 of the project that focused on providing some basic conceptual models and architecture for such a blue print and by relating the interim results with the work in Action Line 2 which focused on experimenting with enabling technologies on diverse platforms (Java and .NET based Web Services), facilitating a scenario-driven integration and proving the feasibility of prototyping critical elements of the architecture. The results of this exercise lead into three main results:

   a. The reference architecture and implementation of six subsystems for the TrustCoM framework blueprint. These are depicted in Figure 1 and they are described in more detailed in section 3.4.

   b. The analysis of the dependencies between the services and the info-sets in each subsystem in order to ensure their best distribution in self-coherent and loosely coupled groups. This has been driven by selected integration scenarios that are orthogonal to the project testbeds, and have served to ensure interoperability and the sufficiency of the subsystems design and reference implementation.

4. Coordination of interactions and collaboration with other European projects. TrustCoM participates in European project clustering activities, and establishes collaborations with other initiatives, in order to maximize impact of the project and avoid duplication of effort.

The following specific collaborations are promoting interoperability of concrete technical work:

a. The GVOA work is promoted within the Grid Trust and Security TG6 technical concertation group, and particularly within the CoreGrid project.

b. TrustCoM adopts the same process model for collaborative business processing as used in Athena and other projects.

c. The SLA developments in TrustCoM are performed in collaboration with AKoGriMo and NextGrid, with specific aspects being pursued further in the upcoming project BREIN.

d. The TrustCoM security token and security token services work is being carried out by EMIC across and in collaboration with the NextGRID and MOSQUITO projects.

e. The TrustCoM secure audit service is being used in a US NSF and a UK JISC project.

f. The TrustCoM policy models have been aligned with UK research projects in the area.

g. Design patterns on Trust and Security and VO Infrastructure are influencing the work of the BEinGRID project in the areas of Secure Federation, Federated Identity Management, Access Control and Application-layer Security Enforcement.

h. There is a close general technical interaction on various aspects with Akogrimo, ELeGi, and GUIDE.

i. TrustCoM influenced the plan of the BEinGRID project with which close collaboration is anticipated.

j. TrustCoM participated at the DG INFSO Enterprise Interoperability Cluster and the Grid Concertation events (via Atos Origin, BT, CCLRC, EMIC and HLRS).

k. TrustCoM contributed to the creation and steering of relevant working groups of the NESSI initiative where several project partners (including Atos Origin, BT and IBM) participate.

A final update of the assessment of the project achievements and recommendations for further research and development will be provided in the final update of this deliverable towards the end of the project (M36) in a public version of this deliverable.

3 Main Research Challenges and Project Scope

Recent years have seen an unprecedented acceleration in the evolution of the Internet as the technological vehicle underpinning the expansion of service provision and inter-/intra- enterprise integration in all market sectors. This brings about the prospect of *ad hoc* integration of systems across organisational boundaries to support collaborations that may last for a single transaction or evolve dynamically over many years. This sets new requirements for scalability, responsiveness and adaptability that necessitate the on-demand creation and self-management of dynamically evolving virtual organisations (VO) spanning national and enterprise borders, where the participating entities (enterprises or individuals) pool resources, information and knowledge in order to achieve common objectives. The objectives may be short term - e.g. to deliver an one-off service in response to a specific customer demand - or long-lasting. In the latter case, the VO's structure, business processes and operational infrastructure must adapt as the goals of the collaboration, the participating entities, the business context and the technologies employed, change.

Emerging ICT paradigms such as Autonomic computing, Utility computing and Grid computing are making the formation and operation of virtual organisations easier by providing dynamic management of the distribution of computational processes across available resources. However, the malleability of the digital medium that makes this possible is also a liability: a major limiting factor is a well-founded concern about exposure to fraud or misuse of the technology. Today, concerns about trust and security are acknowledged to be significant barriers to providing access to outsiders. In spite of the major ICT breakthroughs of the last two decades, protecting one's assets while integrating services, processes and resources, remains a major ICT challenge. Overcoming such challenges requires the development of disruptive technology realising innovative ideas over widely acceptable interoperable platforms. The required scalability, responsiveness and adaptability for on-demand created and dynamic virtual organisations, makes the provision of *cost effective* trust and contract management solutions for VO environments, *the* most demanding and timely research challenge in this field. Effective solutions require interdisciplinary approaches integrating tools from law, cognitive and social science in addition to telecommunications and computing. The successful deployment of *secure* and *trusted dynamic VOs* requires converging strategic research at a European level, coupled with mechanisms for integration of existing experimental results and the rapid dissemination, realisation and take-up of new research outputs.

3.1 Main outputs of the TrustCoM project

In response to this challenge, the European Commission and a consortium of end-users, major software vendors and telecom operators, national research institutes and Universities, are implementing the new Integrated Project TrustCoM. TrustCoM conducts multidisciplinary research in order to deliver:

1. *A novel trust and contract management reference architecture* that will enable collaborative work within on-demand created and self-managed dynamic VOs leveraging on the emerging convergence of Web Services and Grid technologies.
2. A set of *conceptual models* explaining the fundamental concepts, principles and methods underpinning the above architecture. Effectively these provide the meta-model of any new architectural constructs that may result from TrustCoM research.
3. A set of *profiles,* that bring together and potentially extend selected Web/Grid Services specifications at specific version levels, along with conventions about how they work together to support potential implementations of the TrustCoM framework.
4. *A reference implementation of the above* integrating and extending already established or emerging interoperability standards for autonomic security, trust and contract management based on Web and Grid services technology.

5. *System and software engineering tools and methods* analysis of the VO life-cycle and offering a library of design patterns and generic software components implementing selected services that offer the core functionalities of the VO.
6. *Testbeds* exhibiting instantiations of the above architecture and reference implementation into two classes of realistic application scenarios, namely collaborative engineering (CE) and provision of ad-hoc aggregated services (AS).
7. *Selected demonstrators* exhibiting the business value and benefits of the TrustCoM framework in the abovementioned application domains.
8. *Studies analysing selected aspects of the legal and socio-economic context* that underpins such Virtual Organisations.

3.2 Examples of Virtual Organisations

3.2.1 Virtual Organisations in Collaborative Engineering

The development, production and support of modern products such as ships, aircrafts, etc. are highly complex processes that often involve great risk. Principal risks include technical complexity (both in the complexity of products and processes) and changing customer and market requirements. The ability to manage these and other risks is a distinguishing feature of competitive organisations in the engineering sector. A strategy for managing this complexity is to form partnerships or Joint Ventures (JVs) in order to exploit new markets and opportunities through Collaborative Engineering (CE). In a JV partners focus on particular aspects of the product through its lifecycle, enabling more focus on core business capabilities. Emerging technologies such as web and grid computing may facilitate the evolution of JVs into Virtual Organisations (VOs), where organisations quickly come together to share resources without requiring the development of new facilities and systems - a common feature of JVs at present. The CE scenarios described here attempt to cover most of the phases of the product lifecycle within a CE VO through development, production and in-service product upgrade.

In summary, three scenarios have highlighted the importance of effective and flexible security system for building confidence in the extensive and more integrated collaborations that VOs offer over conventional JVs. The security policies should also be correlated both with the collaborative agreements established between partners at the business level and with agreements established within other collaborations as well. The benefits from an effective security and contract management framework are the ability for engineering collaborations to be quickly reconfigured in order to expose the assets that need to be shared to achieve the business goal. Service level agreement monitoring is important for ensuring that suppliers (of components, services etc) perform according to contracts. Benefits here possibly include the automation of processes between clients and suppliers that are usually repetitive. Finally, trust frameworks are required for supporting collaborations. The first of these frameworks concerns managing the reliability and traceability of engineering data, ensuring that greater confidence can be given to it and that it can be relied upon in the major engineering tasks. The second of these Trust frameworks should facilitate the search for new partners/suppliers of components or services that were previously unknown to the VO. This should include some assessment of the trustworthiness of the security systems and its security policies. It has been recommended that TrustCoM focuses initially on the latter area, as a higher priority, where the technology and methods investigated by the Consortium can have a stronger impact, and then address the former as a lesser priority.

3.2.2 Virtual Organisations for Next Generation Service Providers

We are interested here in VOs that are formed through ad hoc aggregation of component services offered by different service providers. Increasingly, enterprises are using web services and related technologies to provide their customers, suppliers and partners with direct access to their services and business processes. Motivations include reducing costs and speeding up processes through

automation. However, the vision behind the web services / service oriented architecture revolution is that distributed applications can be assembled as needed by connecting together pre-existing services. Selection of the services to use takes place through a 'discovery' process. As well as connecting the services together into a supply chain capable of fulfilling a customer order, the business process of the enterprises involved must also be interfaced. Furthermore, contracts need to be agreed that establish the mutual rights and obligations of the participating service providers. When connections at these three levels can be established on demand, we can truly say we have an ad-hoc dynamic VO.

We are already seeing services being 'disaggregated', that is, in addition to offering 'complete' services, simpler constituent services are offered separately. Other organisations can then make use of these constituents in combination with their own service elements to offer composite services to their customers. Motivations for disaggregating include regulatory / anti-trust factors, advantages arising from focus on core competences, business agility (ability to launch new services / enter new markets rapidly), a desire of a part of the individual SPs to retain the advantages of small scale (or conversely to avoid the overheads and inertia of large organisations). New services may also be created specifically for use as constituents of larger services offered by other enterprises. This could offer opportunities for specialist start-up companies to enter the market. Benefits of a dynamic aggregation include provision of services that are precisely tailored to a specific customer need. The need to offer a wide range of tailored services could arise from a wide range of preferences or requirements among the targeted customer base, or because the specifics of the service depend on the circumstance of the customer, e.g. current location, the task currently being undertaken, and other context specific variables. The ability to participate in dynamic VOs greatly increases the range of services a provider can offer to its customers, and also the number of end-customers it can reach indirectly via partners.

Five such 'Aggregated Services' (AS) scenarios have been defined and analysed as part of the TrustCoM problem definition activity. In summary, the five scenarios have highlighted that dynamic VOs inevitably incur a management overhead compared to real organisations, and indeed to static VOs (formal consortia). There is a requirement for additional services to provide the glue that enables the VO to function as a viable entity e.g. to provide overall coordination of activities while retaining flexibility. We expect that these services can be defined in such a way that they are basically independent of the particular application domain. Furthermore, there is a requirement for services to replace the trust inherent in operation within an integrated real organisation (trust in colleagues even when not known personally, trust in procedures and processes, etc.), and the trust between customer and an established service provider with a clear legal identity and brand / reputation. This last class of service is a main ingredient of the TrustCoM Framework. Without such a framework, it is likely that enterprises will judge that the risks in participating in dynamic VOs will out-weigh the benefits. Similarly, end-customers will be reluctant to buy from dynamic VOs. It should also be recognised that there are substantial commercial opportunities for enterprises offering the trust, security and contract management services instantiating the TrustCoM framework. The TrustCoM project will prototype the implementations of potentially useful classes of service, drawing on the scenarios mentioned above for the requirements.

Following the analysis of the five aggregated services scenarios, a presentation of alternatives, and advice from the TrustCoM project reviewers, the Consortium decided to select an AS scenario in the area of eLearning. This scenario tackles the full life-cycle of creating communities of eLearning service and content provision and the process-driven integration of these into an aggregate service that follows a personalised learning path.

The flexibility of TrustCoM is precisely to federate learning services, resources and providers, without having to create a whole infrastructure of security and service-level agreement management each time that collaboration is being set up. Also the learning services and resources are not tightly bound to the infrastructure; they can be designed and developed independently of the specificities of the underlying infrastructure. By taking advantage of this agility it is easy to start providing the services to the Learners, often by reusing existing learning services and resources, while achieving fast-to-market timescales.

3.3 Summary of research challenges & anticipated innovation

TrustCoM aims to develop a coherent framework (architecture, services descriptions, and interaction protocols) that provides means of achieving:

1. *Establishment of trust* relationships by means of digital identities, certification, reputation, and inspection to ensure the security, dependability and competency of the business partners,
2. *Autonomic security*, including the specification, automated management and enforcement of policies controlling fine-grained access to the services and resources contributed by the VO constituents and assuring confidentiality / privacy, integrity, availability and accountability at VO level, while self-adapting to contextual changes within the VO.
3. *Contracting*, focusing on the provision of trusted services to support the management of electronic contracts, the incorporation of guarantees to facilitate trustworthy collaboration, and performance assessment at the enactment of electronic contracts (in particular those related to SLAs).
4. *Business Process Enactment*, focusing on securing the enactment of collaborative business processes invoking services and consuming resources contributed by the VO partners in compliance with their security policies and agreements. Emphasis is also placed on self-adaptation of the business process enactment in response to contextual changes within the VO, including changes to the VO membership, security policy or agreements.

Although innovation in any of the above areas constitutes in itself a significant contribution to Information Society, the *added value of integration* is enormous, providing:

1. A balance between the significance of the business process goals, the expected competence of the contributors, the required level of protection of shared assets, and the terms of collaboration, in relation to the VO objectives.
2. An optimal selection of VO members, based on the goals of the collaborative business processes they will contribute to, their competence for the tasks assigned to them, the policies defining a partner's own terms of involvement, and contracts expressing the mutually accepted context in which collaboration takes place.
3. A sustainable coherence between the efficiency gained by relying on an entity's competence to perform a delegated task, the need to sufficiently protect one's assets (especially when opening-up to collaborators), the necessity to perform and adapt within the boundaries set by potentially incomplete mutually accepted agreements, and the need to take decisions on-the-fly about which task to assign to whom in order to respond in a timely manner to a business opportunity.
4. Continuity and sustainable quality in service provision within VO ecosystems, where evolution is characterised by frequent changes of variable force in the organisational context and short period of relative stability. To ensure that such changes do not damage the equilibrium of complex collaborations between potential competitors, one has to ensure rapid responsiveness to sudden changes in trustworthiness, the ability to swiftly renegotiate and amend agreements and to accordingly adjust security policies, and their enforcement mechanisms.

We expect that some of the enabling technologies are being or will be produced by other projects and initiatives. In such cases, TrustCoM focuses on innovation in terms of holistic integration.

Research and technological innovation in the above themes will be informed by analyses investigating the legal and socioeconomic context of VOs:

5. *Socio-economic Context*. Based on an empirical analysis of the market needs, TrustCoM aims to develop new socio-economic models underpinning the establishment of digital economies within which VOs can evolve and generate profit. These will identify methods for creating incentives for engaging in trustworthy electronic collaborations and sharing services, resources information and knowledge within VOs in order to achieve common objectives in a way that multiplies their productivity and allows for the achievement of results that participants could not produce on their own.

6. *Legal Context*. TrustCoM will study selected legal and regulatory issues of collaborative work in VOs, focusing on privacy, data protection, and international issues. Analysis will also assess the expected impact of technological innovation in light of these issues and some legal and regulatory factors that could influence its exploitation.

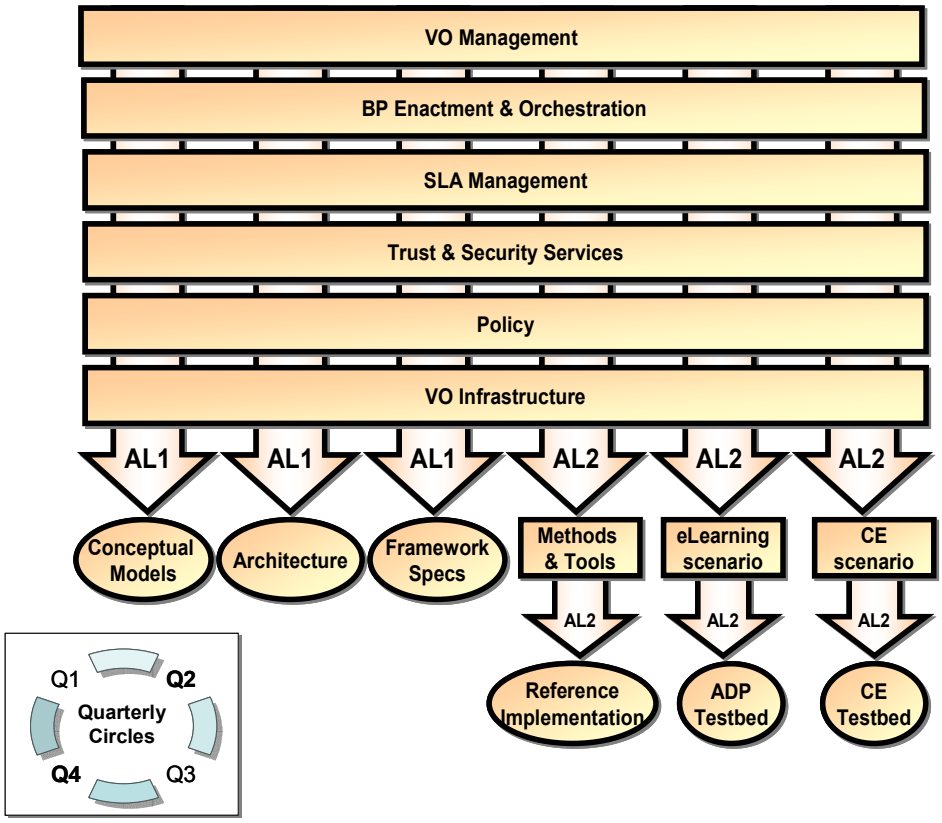


Figure 1: Structure of the project's technical core

3.4 TrustCoM Framework: an overview

The TrustCoM Framework is divided into six loosely-coupled subsystems, each of which focuses on a complementary aspect of an ICT infrastructure for dynamic Virtual Organisations. In this section we provide an overview of the TrustCoM framework. Refer to deliverables on *Conceptual Framework* and *Reference Architecture* [5] and [23] for a detailed description of an abstract architecture proposal, deliverables on *Reference Implementation* [12] and [20] for a description of the detailed designs of the components and services that are currently being developed and to deliverables on *Standards Roadmap* [15] for a detailed description of the open standards technologies upon which the TrustCoM Framework is based.

3.4.1 Enterprise Network versus Virtual Organisation

A starting point for the TrustCoM framework is the requirement for an advanced form of an open distributed and standards based Enterprise Service Bus (ESB) which we have named "Network of Enterprises" or "Enterprise Network" (EN) in order to avoid overloading the ESB term.

In addition to the common ESB characteristics, i.e. being based on Service-Oriented Architecture and having messaging, intelligent routing, and transformation capabilities, we require that EN provides capabilities for brokerage, notification, distributed transactions, security federation, policy

enforcement, and a common service management framework, including the ability to programmatically deploy new application capabilities and to create, and manage the life-time of dedicated endpoint instances for virtualising these capabilities in the context of different VOs.

The EN concept also extends the ESB model by incorporating VO agreement, service-level agreement and policy templates that can be instantiated upon request in order to facilitate the rapid formation of VOs. In analogy to the EBS paradigm, there is a clear separation between the EN, where capabilities are exposed and advertised, and the application hosts that simply accommodate application-specific or supporting components that implement the capabilities. Access to the capabilities takes place only in the context of some VO and only via dedicated, managed endpoints. (At a conceptual level the latter are analogous to service instances of a capability that are offered exclusively to a VO and are subject to the agreements and policies of that VO).

The EN can be understood as the infrastructure underpinning a VO ecosystem. Although the EN/VO Infrastructure subsystem of the TrustCoM framework aims to offer key functionalities of the EN concept described above, all other subsystems of the TrustCoM framework focus mainly on what happens within such a VO ecosystem.

3.4.2 TrustCoM Framework subsystems

3.4.2.1 Virtual Organisation Management

This subsystem aims to offer the essential capabilities for managing the state and life-cycle of a Virtual Organisation. In particular, it defines and maintains details of each Virtual Organisation that is operating within the Enterprise Network and offers three main modules that are respectively responsible for the lifecycle changes to the VO, the VO membership management, and the General VO Agreement management.

3.4.2.2 Business Process Enactment and Orchestration

This subsystem aims to offer the essential capabilities for modelling, deployment and execution of collaborative business processes across a Virtual Organisation. In particular it offers services for producing choreographies from high-level business process models, distributing views of such processes to different VO partners, and for the secure enactment of these processes by services offered by the corresponding VO partners.

3.4.2.3 SLA Management

This subsystem aims to offer the essential capabilities for managing the life-cycle of (Web services) SLA instances among different VO partners and for monitoring the fulfilment of these agreements. Its ultimate goal is to support the full “lifecycle” of a service level agreement between the service provider and a customer, respectively the virtual organization – this covers provision of SLA-related information about a service, negotiation of SLA terms, configuration of the involved components, enactment of the SLA (monitoring and evaluation), feedback, and finally “unbinding” the service provider at the end of the SLA instance life-time.

3.4.2.4 Trust & Security Services

This subsystem aims to offer essential capabilities for security credentials management, auditing and reputation in dynamic Virtual Organisations. In particular, this subsystem contains services for issuing, processing, negotiating and validating credentials assigned to services and resources of different VO partners; services that enable auditing message exchanges within a VO; and services for evaluating “reputation” of a VO partner based on evidence about the performance of the services and resources that are contributed to the VO by this provider;

3.4.2.5 Policy

This subsystems aims to provide the capabilities for defining, managing the life-cycle of, and making decisions at run-time on the basis of, policies that control access to services and resources of VO

partners, policies for delegating (under constraints) the authority to administer specific types of access control policy, as well as of policies for dynamically reacting to changes of the VO context.

3.4.2.6 VO Infrastructure

This subsystem aims to offer the infrastructure upon which the capabilities offered by other TrustCoM subsystems may be deployed. In particular to allow for

- Remotely deploying new business services or TrustCoM capabilities as Web services within an Enterprise Network or an already formed Virtual organisation.
- Creating on demand new VO-specific instances of business services or of already deployed TrustCoM capabilities, and managing of the life-cycle of such service instances through dedicated management services.
- Enforcing specific security, SLA management and transaction actions on VO-specific service instances.
- Dynamically re-configuring at run-time the binding of VO-specific service instances to the trust, security and SLA monitoring components that support their operation without any need for redeployment.
- Dynamically adapting at run-time the enforcement actions applied on VO-specific service instances without a need to redeploy the service.
- Allowing the implementation of secure and reliable message exchange protocols between VO-specific service instances.
- Allowing the implementation of explicitly defined protocols that implement common transactions requiring the dynamic integration of several components from one or more TrustCoM subsystems.

3.5 Projected timescales

Over the last three years we have seen a widespread study and adoption of SOA based approaches in Business-to-Business (B2B) environments. Since the creation of the TrustCoM initiative in 2003 and the beginning of the EU funded integrated project in February 2004, the appreciation and understanding, by the wider ICT research and business community, of the project objectives and of the SOA principles underpinning the TrustCoM framework, has grown substantially. This has been partly because of direct or indirect (e.g. via product groups, consultancy and other lines of business) knowledge transfer from the TrustCoM consortium, and partly because we were right in predicting the evolution of the technology.

The relevance and significance of the TrustCoM research objectives is further substantiated with the recent release (October 2005) of a new SOA maturity model[1] (Figure 3) by innovators in SOA products that include vendors such as Sonic Software, Systinet, and Amber Point, who are not affiliated with the TrustCoM consortium. This model shows cross-enterprise scope as a common characteristic of the top three (out of six) SOA maturity levels. It also emphasises cross-enterprise security, real-time business transformation, and real-time adaptation (i.e. the ability to automatically react and respond to events and contextual changes) as critical technology success factors in meeting the top three SOA maturity-levels. The relationship between SOA maturity and the established classification of the Capability Maturity Model (CMM) levels is summarised in the preceeding diagram (Figure 2).

Few – if any – of today's SOA vendors offer functionality that can be used in order to achieve SOA maturity levels 3-5. We expect that the research results of the TrustCoM project and their realisation over an infrastructure that is build using open standards across all layers – as opposed to vendor

[1] J. Bachman, S. Kline, and B. Soni, A New Service-Oriented Architecture Maturity Model, Sonic Software, Systinet, Amber Point, Bearing Point 2005

specific proprietary solutions – will become a critical differentiator of VO enabling technology that will emerge between 2008 and 2010.

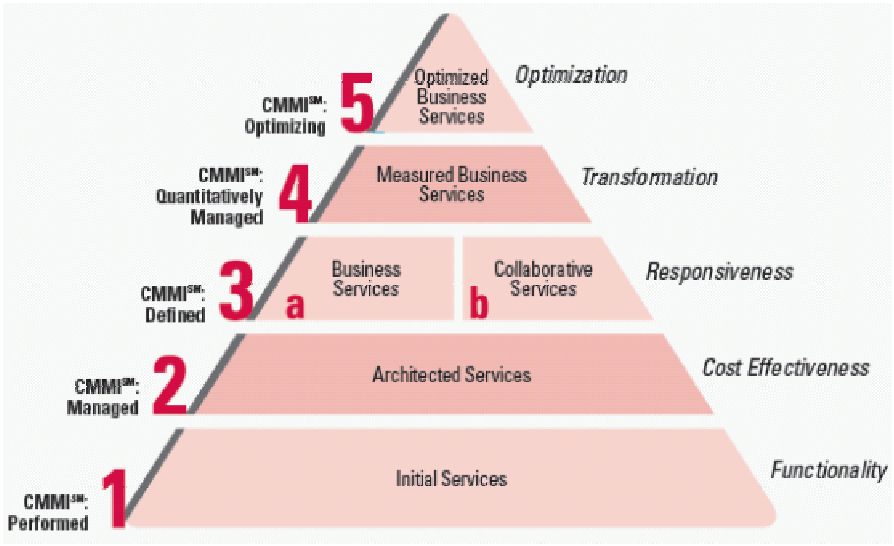
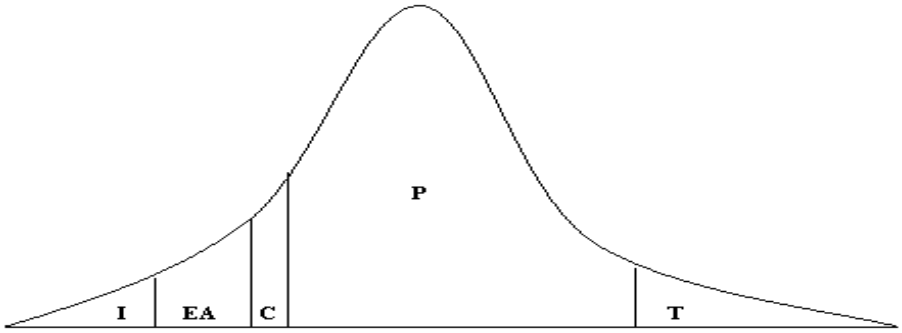


Figure 2: Relationship between SOA maturity levels and business impact expressed in CMMI terms[1]

Maturity Level	Prime Business Benefits	Scope	Critical Technology Success Factors	Critical People & Organizational Success Factors	Selected Relevant Standards
1. Initial Services	New functionality	R&D experimentation, Pilot projects Web site, Portal, Custom integrations, Small number of services	Standards, Legacy Integration	Developers learn service development skills	XML, XSLT, WSDL, SOAP, Java, .NET
2. Architected Services	IT cost reduction and control	Multiple integrated applications	Support for heterogeneity and distributed systems, Reliable Messaging, Mediation, Ease of deployment, Database integration, Versioning, Internal Security, Performance management	Architecture group provides leadership, SOA Competency Center	UDDI, WS-ReliableMessaging, WS-Policy, WS-Addressing, XQuery, WS-Security, SAML
3.a. Business Services	Business responsiveness — change business processes quickly and effectively	Business processes across business unit or enterprise	Reuse, Ease of modification, Availability, Business process rules, Event-driven processes, Composite applications	IT Partnership with Business, Partnership across Organizations, SOA Life-cycle Governance, Executive commitment, Event-driven design skills	WS-BPEL
3.b. Collaborative Services	Business responsiveness — collaboration with business and trading partners	Services available to external partners, Cross-enterprise	External services enablement, Cross-enterprise security, Translation of cross-enterprise protocols, Long-running transactions		RosettaNet, ebXML, WS-Trust
4. Measured Business Services	Business transformation from reactive to real-time, Meet business performance metrics	Business unit or enterprise, Cross-enterprise	Business Activity Monitoring, Event Stream Processing, Complex Event Processing, Event-driven dashboards and alerts	On-going business process evaluation and response	
5. Optimized Business Services	Business optimization — react and respond automatically	Business unit or enterprise, Cross-enterprise	Event-driven automation for optimization	Continuous improvement culture	

Figure 3: Summary of the SOA maturity model[1] released on the 27th of October 2005 by a group SOA-based product vendors (Sonic Software, AmberPoint, Systinet, BearingPoint)

In the rest of this section we summarise projections indicating the timescales within which we expect the areas where TrustCoM is making research advancements to have an impact. We do this by means of three diagrams: the projected impact of the technologies relating to the TrustCoM subsystems, the projected timescales of the standards adoption relating to the TrustCoM Framework and the projected timescales by which the research advancements tackled in each TrustCoM subsystem are likely to have an impact. Instead of absolute timescales our diagrams have been normalised in relation to the following distribution.[2]



Innovators (I)	The enthusiasts who like technology for its own sake.
Early Adopters (EA)	Those who have the vision to adopt an emerging technology to an opportunity that is important to them.
The Chasm (C)	Time gap in technology adoption, which is between the early adoptors and the pragmatists.
Pragmatists (P) Early Majority	Early majority pragmatists are the solid citizens who do not like to take the risks of pioneering, but are ready to see the advantages of tested technologies. They are the begining of a mass market.
Pragmatists (P) Late Majority	Late majority pragmatists, who represent about one-third of available customers, disklike discontinuous innovations and believe in tradition rather than progress. They buy high-technology products reluctantly and do not expect to like them.
Traditionalists (T)	Traditionalists (laggards) do not engage with high technology products - except to block them. They perform the valuable service of pointing out regularly the discrepancies between the day-to-day reality of the product and the claims made for it.

Figure 4: Overview of Moore's high technology product adoption pattern and adopters' classification

[2] The distribution is based on the elaborate analysis on trends underpinning the introduction of new technology by Geoffrey Moore in *"Crossing the Chasm: marketing and selling high-tech products to mainstream customers"*.

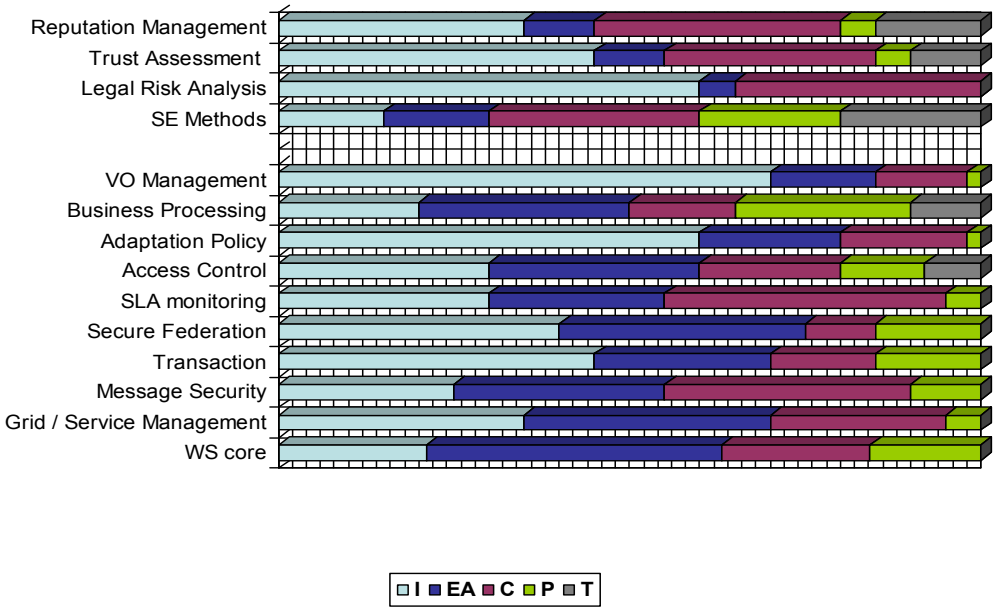


Figure 5: Applied research results uptake normalised over Moore's distribution.

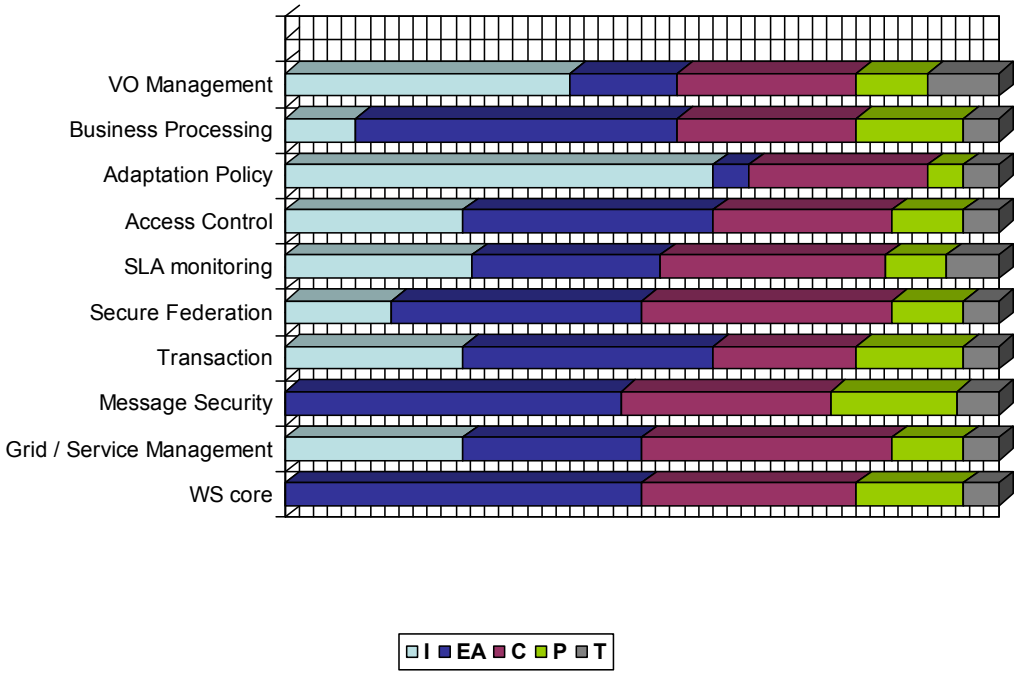


Figure 6: Standards adoption normalised over Moore's distribution.

4 Progress assessment & recommendations: *technical core*

In this section we provide an updated self-assessment of the project progress against our detailed scientific and innovation related objectives and offer recommendations about improvements for the remainder of the project and for further research after the end of the project, where appropriate. The section is structured as follows: there is a subsection for each project aspect (i.e. six technology focused aspects, one related to technology integration and two contextual) where we revisit the main objectives in more detail, and then we summarise progress against these objectives and offer recommendations for further work.

4.1 VO Management

4.1.1 Detailed objectives and research challenges

Existing work in VO Management focuses on maintenance of members and issuing of credentials to allow access to distributed resources. We however view this as insufficient to address flexibility and automation challenges required for spontaneously formed VO's that address specific business objectives. A comprehensive, distributed system architecture is required, along with management interfaces and protocols, in order to achieve truly dynamic VO management.

We have identified the following research challenges relating to VO management:

- *VO Specification* – integrated services and management interfaces for specifying collaborative business processes, membership roles, service level agreements and event-condition-action policies
- *VO Identification* – searching for potential members and exchanging relevant documents (i.e. those required for immediate configuration of systems, e.g. choreography, service level agreements, policies) via invitations. These different documents should be associated with a higher level document called the general VO agreement (GVOA). Services and management interfaces for managing these documents need to be made available for authorized members and administrators of a VO and its infrastructure.
- *VO Formation* – automating the process of configuring the enforcement points, services and processes of each member, as well as providing message-based notifications when all members are prepared for execution of the agreed collaborative business process.
- *VO Operation* – this involves the interfaces for starting a business process, given all members are ready. Members and users should be provided with feedback concerning the status of the process and VO. Secondly, there is a need of ensuring that members only gain and provide access to resources when this is required, according to the control and interaction flow of the collaborative business process.
- *VO Termination and Member Replacement* – protocols and management interfaces for ensuring that, when members are replaced or the VO is terminated, there is no access to resources strictly reserved for usage within the VO.

4.1.1.1 Emerging solutions and trends

Again, VO management is a term that has a very specific meaning with respect to maintaining the association of members and permissions in a resource sharing environment such as in the Grid (see CAS www.globus.org/security/CAS/ and VOMS http://infnforge.cnaf.infn.it/projects/voms/). The solutions presented in TrustCoM extend these primitive notions, by comprehensively integrating

Membership Management, Business Process Management and Access Control. These lead to potential gains in automation and flexibility of management for dynamic VOs.

- *VO Management Architecture and Service Components*: we have proposed a model consisting of three service groups (Host, Initiator and Member), which serve to simplify the installation of pre-configured service-oriented software for different types of VO management responsibilities.
- *VO Management Interfaces*: we have developed a graphical, web-based means of using the respective VO management services, as well as supporting services, in order to facilitate human interaction in the specification, identification, formation, operation and termination phases of a VO
- *VO Management Protocols*: we are designing protocols for securely inviting members, executing the choreography as collaborative business processes and handling exceptions – this requires integration with the business process and security subsystems
- VO Access Control Policy Generation: we have developed a means of generating the minimal access controls for a choreography, such that the authorizations are available at the time of executing the collaborative business process.

4.1.1.2 Open standards and common design patterns

There are no open standards technologies addressing VO Management as such. The following technologies address aspects of components that may be contributed to the development of VO Management services, protocols and interfaces:

- UDDI technology provides the basics for service discovery and integration. The standards for representing and uniquely identifying business entities have been incorporated in the identification and formation phases of VO management.
- XACML (eXtensible Access Control Markup Language) is assumed to be the target language for generated policies, maintaining compatibility with the other components in the framework that manage authorizations at different levels.

We reviewed and considered ebXML incorporation in our architecture but did not pursue this, although motivated by some pre-existing concepts - see section “3.1: VO Management” of [15].

4.1.2 Project assessment

The VO management of TrustCoM includes the first implementation of a management architecture spanning the entire life-cycle of VOs providing services and protocols for each of the phases, called the VO Management Toolkit. It provides a unified GUI management interface supporting the administrator to easily handle all aspects of VO management. Furthermore, it offers a high degree of automation as exemplified by the Policy Generator greatly reducing management efforts.

Virtual Organization Management Toolkit: The VO Management Toolkit development goals are to provide services, tools and interfaces required to create an on-demand VO. It is considered as complementary to the Enterprise Network support tools, in that it was developed with a top-down view on the application support required for an on-demand VO. The toolkit is deployed as three distinct components, called editions. These editions bundle the functionality as required by different companies within a VO:

- The “Host Edition” provides VO-wide services such as member registration and monitoring of VOs. It is the central place of storage for VO databases and services.
- The “Initiator Edition” allows the creation of VOs. It provides the user interface to all services required for managing a VO. It can trigger all the changes in the lifecycle of a VO.
- The “Member Edition” allows the participation in a VO. It stores the state of the member in each VO and provides basic communication services.

The lifecycle of a VO contains four phases which are covered by the toolkit’s management services and protocols. In the “Identification” phase a new VO and its business goals, workflow, policies and

SLAs are defined. During the "Formation" phase potential member candidates of the VO are searched, combined and assigned to their individual roles. During the "Operation" phase the business workflows are executed to achieve the actual business goal of the VO. In particular this means that the companies' services are executed as part of BPEL processes generated out of WS-CDL data defined in the first phase. The current state of the VO can be monitored with the toolkit during this phase. Finally, in the "Dissolution" phase the VO is dissolved.

It is intended that the Toolkit can be used as a test system for simulating the on-demand creation and operation of virtual organizations, integrating the functionality of the various components and subsystems developed in the TrustCoM project. This includes the user interface required for administration of a VO throughout its lifetime, as well as the integration of the various services required to secure and monitor the reputation and contractual-compliance of interactions in the VO. Ongoing work on the toolkit are enhancing its administration and security.

Policy Generator (PGC): The policy generator is an optional tool a security administrator of a VO's member organization can use to decrease the effort of managing the security of his organization's services in the VO. The input of the policy generator is the agreed choreography of the VO's business process in WS-CDL format. The output of the policy generator is a set of access control policies in XACML format that allow access to its services to the calling members in the VO.

The guiding design principle of the policy generator is the least privilege principle, in that only such policies are generated that are necessary for the fulfillment of the business process, i.e. removing a policy from the set results in an access violation during the enactment of the choreography. The security administrator can then employ a simple administration model: All accesses to his services are denied, i.e. there are no policies in place. Whenever a VO is being created, the policy generator will create the minimal policies necessary to allow the VO to operate. Furthermore, since all policies grant access there are no conflicts.

The policy generator has been integrated into the VO Management Toolkit and seamlessly works in the VO lifecycle model. After the choreography has been agreed and all VO members have been selected, a request to the local VO administrator is made to call the policy generator. This call is optional and if denied it is the administrator's obligation to install correct access control policies. If the policy generator is being invoked the administrator has the option to review the policies before deployment. The benefit for the security administrator of using the policy generator is that it replaces the manual policy creation, administration and verification process with the click of a button. It lifts the management effort from the technical process of creating access policies to the business level of choreographies.

4.1.3 Recommendations

VO management as defined and used in TrustCoM enhances the notion of VO management in other projects as described in section 4.1.1.1. The TrustCoM VO toolkit is the first attempting to integrate to aspects from all phases of the VO lifecycle in one management subsystem.

The main remaining key challenge in the area of VO management for the remainder of the project is to prove the validity and practicality of the developed implementations and concepts by applying it to the testbeds and, where appropriate, the business demonstrators. This requires the finalization of the schema for the General VO Agreement, which contains and correlates all VO-level necessary agreements, and the integration of the policy generator with the policy subsystem and the concepts for access control developed in TrustCoM. Particular attention should be placed on VO management behaviour in case of VO adaptation in response to contextual changes during the operation of the VO and its automation, as well as the seamless integration of business processes into the VO lifecycle.

4.1.3.1 Areas of further research and knowledge transfer

Topics of further research after the end of the project include:

- The recommendation of a profile for the General Virtual Organization Agreement and the definition of widely accepted protocols for coordinating and managing the life-cycle and state of a VO.
- The enhancement of the VO management subsystem in order to allow the simultaneous life-cycle management of different VOs that can be formed and evolve within the same network of enterprises. This is particularly important, for ensuring the uptake of the VO management capabilities conceived in TrustCoM and for facilitating dynamic virtual organizations.
- The enhancement of service provisioning and management toolkits (such as those offered by Computer Associates, IBM and SAP) and of customer relationship management products and application hosting products (such as those offered by SAP) with VO management capabilities.

4.2 Business Processing

4.2.1 Detailed objectives and research challenges

There are various emerging and mature standards for Business Process Modelling and Execution. There are however particular challenges that arise in the special context of dynamic, on-demand VOs, which are being tackled by the TrustCoM Consortium.

- *Supporting the life-cycle of Business Process instances*. A major challenge is the integration of a VO-wide collaborative business process with the lifecycle of the VO. Besides the problem of consistently modelling such processes, the extraction and distribution to process views to VO partners and the joint enactment of such processes are particularly challenging.
- *Correlating Business Processes and Service Level Agreements.* As it is elaborated in TrustCoM deliverable **D2: State-of-the-art evaluation,** few (if any) of the existing studies properly tackle business processes in conjunction with SLA and none in conjunction with trust and reputation information for service selection and composition.
- *Supporting adaptation & administrative processes.* As members are replaced and other exceptions occur, it is required that the collaborative processes can be returned to a normal state of execution.

After an initial phase of defining and implementing the core business process functionality, the efforts should focus on three aspects: integration with the SLA infrastructure, leveraging the availability of trust and reputation for providing enhanced flexibility in the enactment of the processes especially across administrative domains, and offering models and technology for automating common transactions between the infrastructure and supporting services that TrustCoM develops.

4.2.1.1 Emerging solutions and trends

By comparison, 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 the 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),

- WS-CDL 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. Meanwhile, development of the BPML/WS-CI has been abandoned with most of the concepts being integrated in a new specification, WS-CDL. At present WS-CDL is also not adequately catering for a collaborative business process choreography description capturing complex message exchanges across administrative domains, for instance in tendering and quotation processes. We anticipate that, as the experiences of TrustCoM partners with the use of WS-CDL for cross-partner choreography grows (especially following the application of choreography in the business scenarios), they will be offering feedback to the WS-CDL community and product vendors in order to help addressing the current shortcomings of WS-CDL.

Finally, there are few solutions, if any, that attempt to tackle the problem of relating business processes with the SLA of the services they engage. Furthermore, the co-use of choreography approaches (e.g. WS-CDL based approaches), which naturally fit for describing high-level VO-wide processes and WS-BPEL (a.k.a BPEL4WS), which naturally fit for implementing more dynamic processes within the realm of a specific VO partner, has not been investigated adequately although it has been often discussed.

4.2.1.1.1 Open standards and common design patterns

- *WS-CDL:* This process choreography language is used to define a collaboration definition for a VO. Based on this collaboration definition, the public business processes and WSDL interfaces of the VO members are derived. However, WS-CDL is still evolving. Nevertheless, it seems to be most promising for specifying the collaboration definition (business protocol) of a VO. It is not complete to cover all complex business interactions (e.g. multicasting). However, the current version of it can be used to base the TrustCoM development upon it. Future versions of the specification will be monitored for further developments.
- *WSCI* is also relevant but we have noticed that WS-CDL to a large extend covers those aspects of WSCI functionality that appear to be more relevant to the TrustCoM goals.
- *WS-BPEL (a.k.a. BPEL4WS)* provides a reasonably mature language set for executable business processes. It focuses on the control and orchestration aspects of business processes and leaves business logic to invoked web service implementation. WSBPEL can be used to specify “public” processes (views) of VO members.
- *BPML* is also relevant but it appears that WSBPEL covers the necessary BPML functionality for the needs identified in TrustCoM.
- *WS-Coordination* and *WS-AtomicTransaction* are used as a means of implementing distributed transactions and coordination protocols at the level of VO Infrastructure. Mechanisms developed in this subsystem for Business Process Enactment will leverage on the VO Infrastructure capabilities wherever such protocols are required.

4.2.2 Project assessment

The main achievement of the Collaborative Business Processing research has been the development of a tool CDL2BPEL that derives executable BPEL (Business Process Execution Language) from WS-CDL (Web Services Choreography Definition Language). This enables the initiator of a VO to specify an overall schema of how members should interact in order to achieve an agreed business objective. Secondly, it allows each member to reduce the preparation time before

being operational within the VO, thus contributing towards the ultimate goal of on-demand VO formation. This is discussed in relation to the three research challenges below:

- *Supporting the life-cycle of Business Process instances*. Each business process has a lifecycle of specification, distribution, formation, operation and termination, corresponding to the VO lifecycle. CDL2BPEL improves the automation of this process, using two 'standard' languages for which interpreters and execution engines already exist.
- *Correlating Business Processes and Service Level Agreements.* There are three extensions to CDL2BPEL called the TSC Context, TSC Role and TSC Task, for representing Trust (T), Security (S) and Contract (C) conditions in the processes themselves. A specification for these has been included but not explored in significant detail in the project. It is however possible for a Choreography to be annotated with TSC requirements (in the form of TSC Roles to be supplied by Partners), which become translated into TSC Contexts and Tasks associated with the BPELs of each member. SLAs are hence managed independently of the business processes (see SLA Management and GVOA).
- *Supporting adaptation & administrative processes.* Each member in a VO is free to define their own private processes, including compensation and adaptation handlers. Once there is compatibility with the public process (i.e. the choreography) these can be realizations of so-called "silent-actions" and need only be specified in the CDL2BPEL Knowledge Base (KB)

There is still some remaining integration and testing to be done with this technical capability, especially the ease with which it is initially set up. With respect to the focus on trust, contract and security management, the contributions of CDL2BPEL tend to be beyond the scope of these and extend to the general area of business processing. However, it can be stated that a choreography represents a contractual commitment between members, while the formal specification of interaction flow is useful for determining the limited access to resources to be granted for involvement in the collaborative business process.

4.2.3 Recommendations

As a VO is formed in response to a business objective that can not be addressed by just one partner alone, a swift reaction to the emerging business need, fast partner consortium formation, and quick, automatic adaptation of IT infrastructures are of essence. Thus, an automated solution deriving executable business processes from a Choreography was desired, following a top-down approach which is aligned with the VO formation and partner selection processes. Business application logic is hereby encapsulated in service implementation. Therefore, a business process at one role can be seen as the ordering structure around local web service invocations, also called orchestration. Orchestration captures the local, role specific view on business processes, which orders the calls on available services and guarantee a defined execution order. In contrast, the global view encompasses the collaborative business process, which orders the interactions between the involved roles. The overall goal of this tool is thus a conceptual mapping that shows how the transformation of a choreography in a standard language to a set of orchestrations in another standard language can take place. The mapping forms the basis for a prototypical implementation, showing the validity of the developed concept. For a given choreography, the orchestrations generated by the prototype then need to be deployed in execution engines and are thereafter executed whenever the need for the collaboration arises. Deployment and execution are the requirements from the VO environment and put a high burden on the semantic correctness and completeness of the orchestrations.

In TrustCoM, the collaborative business process model is based on business partner views. This approach follows established theoretical models, as well as the specifications of the WfMC3. The needs for confidentiality of entire processes or workflows of the respective partners and the integration of multiple private workflows into a global view are identified as critical for successful operation of virtual enterprises, extended enterprises and Virtual Organizations. On one hand, an organization participating in a VO may not be willing to share detailed information about a complete business process, since the information in it represents an asset to its owner. On the other hand, enough information has to be provided to the VO in order to achieve a coherent and stable public workflow. Such an approach introduces a coalition model with three tiers: private processes, public

views of these processes, and a (global) public process. These three tiers correspond to the notions of private business processes, the interfaces of these processes, and choreographies, respectively. Applying the collaborative business process model to the VO environment, the collaborating members are informed about the VO objective through the shared choreography. They can thus infer the behaviour that is expected from them during the VO operation phase which corresponds to their public process. A partner is only required to expose the public process to the VO which serves as the interface for the confidential private process.

Following the Service Oriented Architecture (SOA) paradigm, implemented modular pieces of application logic are assumed to be available as services. Therefore, the private business process can be seen as a stateful wrapper around the services, guaranteeing the defined order of calls to the services. Thus, it is also called orchestration, providing a local, role specific view on a private/public process pair, in contrast to the choreography which captures the global view on a collaboration among different roles. The problem thus is to find a way to generate a set of executable, private processes and the public view on them from a choreography description of the overall collaborative process. Two related problems, that are yet to be fully addressed, which are of major importance for the achievement of the overall goal, are

- identifying the appropriate level of detail for private processes and for public views / choreography, and bridging the the information gap between them, and
- developing appropriate descriptions of private process and public views and successfully correlating these languages.

4.2.3.1 Areas of further research and knowledge transfer

Topics of further research after the end of the TrustCoM project in this area include:

- *More Intelligent Mapping between Silent Actions and Private Processes:* the Knowledge Base is required for completing the mapping between CDL and BPEL. However there are many assumptions made about semantic mappings between the languages, which could be relaxed by more elegant ontological models.
- *CDL Validation and Auditing:* it may be desirable for Initiators and members to audit the execution of VO collaborative business processes to determine that they have been correctly executed as agreed to in the specification.
- *The TSC (Trust, Security Contract) Concept*, i.e. the definition of enforceable constraints for trust and security and contract relation actions to be performed by VO partners: As this concept has been implemented but not fully tested in the project, it would still be worthwhile investigating applications where the concept applies. For example in application hosting it may be the case that an Initiator (who is a process and resource owner) will want to specify their TSC requirements at a high level, enforcing that they are realized by selected members.

4.3 SLA management

4.3.1 Detailed objectives and research challenges

In relation to SLA and contract management, the main research challenges that have been identified are the development of models and mechanisms for the specification of contract templates and the negotiation, monitoring and enforcement of collaboration agreements between existing or prospective VO members. Particular emphasis should be placed on ensuring that such agreements are in harmony with the trust and security management policies across a VO and that they provide a context for the definition and enactment of collaborative business processes across a VO.

In addition to the GVOA, which has been judged as being more relevant to VO management than the SLA subsystem, we have identified research challenges relating to two main types of agreement that applies to VO partners:

- *Category A*: Research challenges related to providing support for managing legal contracts between organisations and automate part of the process associated with their definition and enforcement.
- *Category B*: Research challenges relating to – typically bilateral – agreements that capture customer-provider relationships and the Quality of Service promise associated with the provision of a (Web-) service.

Following the problem analysis and technology evaluation presented in deliverables **D3** and **D2**, respectively, the following specific research challenges have been identified:

- To develop an explicit conceptual model for supporting agreements at both business and service level. This can be based on a fusion of elements of WSLA, WS-Agreement and relevant concepts from more generic contract architectures such as the BCA developed at DSTC.
- The development of this conceptual model needs to devolve significant efforts to two aspects: a) the impact and use of trust and reputation relationships, as well as QoS parameters in service discovery; the negotiation of SLAs and b) the handling of SLA violations in a more flexible form.
- In conjunction with the legal team in TrustCoM, to identify which elements of contract management 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.
- To identify specific design patterns and implement services for the discovery on basis of SLA templates, negotiation of SLA terms, creation of SLA instances, high-level SLA evaluation and infrastructure-level monitoring mechanisms to support the enactment of (Web-) SLAs.

Given the immaturity of solutions to support contracts that fall in *category A*, including the lack of standardised representations and of mechanisms facilitating operational support for such agreements, and taking into consideration the background, commercial interests and expertise of the members of the consortium, we have decided to start tackling research challenges relating to contracts that fall in *category B* before considering the former.

4.3.1.1 Emerging solutions and trends

The BCA architecture[6] is one example of a comprehensive ICT model for dealing with legal contracts comprising sophisticated means of describing contracts as well as processes for contract arbitration and enforcement. However, such frameworks are rather complex and there is virtually no implementation available. Most importantly, they have not been used outside relatively restricted research environments. From a conceptual viewpoint, however, such frameworks propose a number of solutions that are 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 specify 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 concern: specifying SLAs and associating them with the corresponding WSDL services, discovering and locating services based on profiles of QoS that can be maintained by those services, defining simple protocols for negotiating QoS parameters, and monitoring the compliance with the SLA objectives (including 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, which has not been evolving as rapidly as the community had initially anticipated.

ebXML Trading Party Agreement and Collaboration protocol Agreement also offer an attractive alternative baseline. However, their specifications and implementations are tightly coupled to the other ebXML specifications, which predated recent developments in Service Oriented Architectures and often do not integrate well with the more recent web service specifications.

4.3.1.2 Open standards and common design patterns

The following open standards technologies are related to the research challenges mentioned in this subsection and may offer part of the baseline used by the TrustCoM consortium.

- *WSLA*: The WSLA specifications allow for the definition of QoS service parameters and the relationship between involved partners and so-called supporting parties that may take over monitoring, evaluation and related functionalities.
- *WS-Agreement*: As opposed to WSLA, WS-Agreement focuses on interaction protocols and provision of templates. WS-Agreement has little or no support for the definition of QoS parameters. Notably, there seems to be a strong interest by IBM (the developer of WSLA) to integrate WS-Agreement and WSLA.
- *ebXML CPPA*: ebXML CPPA is strongly integrated into the ebXML set of specifications, and may hence not be directly used without significant impact on other technologies used in TrustCoM. However some the concepts used in ebXML CPA appear to be very relevant to the objectives of the project. Such concepts will be adopted following adaptation where appropriate.

4.3.2 Project assessment

Service Level Agreements can be considered as restricted electronic contracts with a particular focus on specifying the conditions and terms with respect to parameters that should be constantly monitored. Similarly to contracts and related to the lifecycle of a Virtual Organisation, SLA support should cover the following main aspects:

1) Definition of SLAs on basis of business requirements
2) Provisioning (publication) of SLA-related information about a service
3) Identification of services based on QoS parameters
4) Negotiation of SLA terms (including verification of resource availability)
5) Configuration of resources according to the agreed upon SLA
6) Enactment of the SLA (monitoring, evaluation and “enforcement”)
7) Unbinding of the involved parties

Current approaches to Service Level Agreements, in particular WSLA and WS-Agreement, generally do not cover the full range of these aspects so that one of the main tasks for TrustCoM consists in building a unified specification and reference implementation that caters for all issues equally.

The SLA Management workpackage has particular focused on the following main aspects:

Conceptual Model for SLA management:

State of the art approaches towards Service Level Agreements do not take the wide range of business requirements into consideration. With respect to the business specific contract terms, the SLA Management workpackage, in cooperation with workpackage 8 (Socio-economic issues) and partially with workpackage 9 (legal issues) examined means of defining more accurate document structures that covers not only the typical performance related information, but the full range of: cost, quality, delivery metrics, analysis metrics and procedures, as well as management issues. The structure is being defined with keeping the relationships between contract management and reputation on the one hand, as well as policy definition. Accordingly, the document structure allows for seamless integration into the overall TrustCoM framework.

Regarding the participant structure, current approaches towards SLAs assume the existence of one single document to cover the full range of contract related requirements, i.e. covering not only the

actual terms and contractual partners, but also the means of accessing and calculating the data; furthermore, published SLA information (templates) is identical to actual SLA documents. Such schemata do not cater for privacy and production cycle / infrastructure hierarchy issues typically connected with business entities. In TrustCoM, we assume that typical VO participants provide abstract "products" rather than simple "atomic" resources, meaning that for each transaction with this entity, a whole business processes may be triggered that actually aggregates the provided functionality (respectively "product") from a variety of sources. Implicitly, most SLA status information is actually aggregated and derived from multiple sources – even though current schemata cater for aggregation metrics, they fail to consider that service providers may not want to publish such information for confidentiality reasons. This issue obviously applies to documents and templates in the same way. Similarly, the status information may be subject to confidentiality issues when being provided to third parties e.g. for evaluation purposes.

Conceptually, we thus foresee a hierarchical model of interdependent SLA document structures covering the individual issues of the respective application area, thus allowing for more autonomous and full range support. Note that no full schema has been devised as yet.

SLA schemata: The SLA schema defined in TrustCoM covers more of the conceptual issues mentioned above than most current specifications and allows seamless integration with the TrustCoM specific framework issues, like reputation scoring and policy evaluation. However at the time of writing, the schema still does not cover the hierarchical structure as conceptually introduced.

SLA subsystem architecture: An SLA Management framework has been developed that greatly enhances the recommendations of current specifications with respect to flexibility and extensibility, in particular keeping the business requirements in mind. As such, the SLA Management subsystem builds upon a Service Oriented Architecture approach that allows for hierarchical structures by simply extending the component distribution, i.e. multiple monitoring facilities may be exploited to hierarchically gather and convert status information and evaluator-monitor-combinations may extend this capability to generate comprehensive performance information.

Since TrustCoM addresses issues related to automated configuration and enactment as required for VO operation, the SLA Management framework also supports manageability of distributed SLA components that are connected by the specifications in the according SLA document (i.e. equally covering signatory and supporting parties) – this allows for quick and easy setup of all parties from a central management point. The local management components may be easily adjusted to individual infrastructure requirements.

Reference implementation of a subsystem structure for SLA enactment:

The basic functionalities, covering setup, monitoring and evaluation have been implemented and have been successfully tested. With the exception of ETTK, which provides only limited support and hardly any flexibility, this belongs to one of the few working and readily available implementations of an SLA Management framework based on WS-Agreement. The implementation integrates and interacts with the related subsystems of TrustCoM, namely the Notification subsystem for message (status) distribution, the Policy subsystem for triggering consequences from evaluation and finally reputation to serve both as status information source, as well as for scoring SLA related performance.

SLA Management is of interest in any business relationship as it provides the means for ensuring quality of service based resource provisioning. Basically, the key actors and their respective benefits from general SLA Management can be enumerated as follows:

- *Application Service Providers:* By enhancing the services with SLA Management support, a business entity may not only reach a wider market by providing quality controlled services, but also make use of self-management capabilities through monitoring his/her own resources and constantly evaluating their status with respect to previously specified parameters.
- *Consumers (including other Service Providers):* Consumers get some control over the quality that is provided by the services they consume. SLA Templates allow for identification of service providers on basis of the quality their resources can maintain. Negotiation capabilities ensure that the contractual terms and conditions meet both the consumer's and the service provider's interests. Monitoring and evaluation provide the means to constantly supervise the resource

status with respect to the previously agreed upon SLA parameters and summarise the status information report-like. Integration with Policy subsystems enables the autonomous enforcement of SLA terms

- *New types of Service Providers (Trusted Third Parties)*: The SLA Management model allows for new types of business entities that provide the supporting capabilities for SLA Management, like integrative Monitoring, Evaluation and – implicitly – Policy Management. Furthermore, SLA Template repositories may be provisioned similar to UDDI registries.

4.3.3 Recommendations

By the end of this project, we want to be able to support the full "lifecycle" of a service level agreement between the service provider and a customer, respectively the virtual organization – this covers provision of SLA-related information about a service, configuration of the involved components, enactment of the SLA (monitoring and evaluation) and finally "unbinding" the service provider again. This will allow service providers and consumers to offer, respectively exploit, services that meet a specific quality of service and to ensure that this is maintained during enactment.

We furthermore want to enable service providers to manage their services with respect to a specific quality. However, TrustCoM will only deliver the basis for this and not examine the required intelligence of such an autonomous self-management component.

To realize these issues, we pursue the following goals:

- Extend the SLA template schema so as to allow for discovery of services on the basis of a quality of service description and to act as a premise for negotiation
- Support notary services with the ability to plug in various SLA signing protocols
- Integrate the SLA lifecycle with that of the VO, exploiting the relationship with the General VO Agreement (GVOA) and including the discovery and negotiation of SLA Management services in the corresponding VO phases.
- Finalize the implementation of an SLA Manager capability that allows for automatic configuration (i.e. binding and "unbinding") of the involved components based on the agreed upon SLA. An SLA Manager will in fact take the form of an aggregation of management services, operating on different administrative domains.

4.3.3.1 Areas of further research and knowledge transfer after the end of the project

The relationship between SLA obligations and business rules in terms of common foundations, common semantic representations and common enforcement and monitoring mechanisms will not be fully addressed in this project. Investigating such a relationship has been among the initial objectives of this project and it is important for fully tackling its original research challenges. However the limitation of resources combined with the immaturity of open source technologies for monitoring the execution of simple contracts such as (Web) SLAs, necessitates reducing the ambition of the original research objectives in this area. Nevertheless the Consortium recognizes the importance of this research objective and recommends that the wider ICT research community supports further research in this direction. Such research will also have to take the legal implications of technology-driven automation into account.

With TrustCoM focusing on the conceptual architecture and reference implementation rather than on issues of semantics and automated reasoning, one category of issues to be solved rest in particular on SLA Negotiation related issues. In order to identify the optimal configuration of SLA Parameters with respect to a) the individual resource's capabilities and availability on the service provider side and b) the customer's business needs on the other side, the Negotiation components need to be capable of weighing "business objectives" versus intelligent resource management capabilities. Even though human intervention may be desirable for negotiation purposes, such a Negotiation component should nonetheless support the task by aggregating status related information in a way similar to the monitoring components (i.e. according to the respective infrastructure) thereby taking

different resource configurations into consideration. This implicitly relates to the issue of mapping SLA parameters intelligently to resource configurations depending on the local infrastructure. Though configuration sets may be exploited for typical parameter-setup-relationships, the actual details will vary depending on the flexibility allowed during negotiation and the manageability of the actual resources.

4.4 Trust & Security

4.4.1 Detailed objectives and research challenges

Federation services underpin the life-cycle of a Virtual Organisation. They enable the establishment and conditional propagation of trust among VO partners and they facilitate the security of the interactions between the services offered by providers participating in the same VO. Often a federation directly corresponds to the Circle of Trust underpinning a VO and security token management underpins the identity brokerage and identity management model of a VO by enabling the creation of virtual identities and the association of business roles and operational roles with these virtual identities.

Trust Management models support the supply and collection of evidence or derived information about the trustworthiness of a prospective VO member to perform a specific task towards an objective of the VO, and the assessment of their reputation by other VO members, who will have to rely on that prospective member (or not) for the specific task.

In order to tackle more effectively this extensive area and to identify common functionalities (such as enforcement, adaptation policies and reputation), which may be of a more generic nature than specific to security, we have decided to divide these research challenges into the following areas:

- Specific research challenges relating to security token services, which includes basic mechanisms that underpin credentials management and offer a foundation of federated security realms of different VO members. These include the development of specific ***"security token services"*** and mechanisms for issuing, validating and exchanging security claims.
- Specific research challenges relating to "**trust negotiation"**, including policies that guide the incremental disclosure of credentials that are needed for satisfying a minimal set of requirements for a particular transaction within a particular VO, and protocols for securely implementing such exchanges of credentials.
- Specific research challenges relating auditing. These include the development of an archetype of an "***audit service***" for VOs and mechanisms that underpin the collection and dissemination of evidence about transactions between VO members.
- Specific research challenges relating to reputation management. These include the development of the archetype of a **"reputation service"** for VOs, of models for meaningfully quantifying reputation and computing reputation values as well as mechanisms for collecting and collating evidence or other information (e.g. recommendations) on the basis of which the performance of a VO partner may be assessed.

4.4.1.1 Emerging solutions relating to federation

Security aspects of a VO framework span a large number of concerns that broadly divide in the following categories: Secure Federation, Authorisation, and Adaptive Security. In this section we focus on the former, while section 4.5.1.1 focuses on the latter two. Overall security and policy are not only a substantial part of TrustCoM but one where the consortium has considerable expertise.

Few of current commercial of experimental middleware platforms focus on federation. Most – if not all – of these middleware platforms do not support recursively composable VOs in federated structures (i.e., a Liberty circle of Trust, or a WS-Federation circle of trust, or a VOMS Grid is

typically *not* 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. 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.

4.4.1.2 Emerging solutions and trends on security and 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 to (or derived from) different elements such as: recommendation, reputation, risk, and evidence of behaviour.
- Trust is linked to a well identified context, which 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 should be 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.

4.4.1.3 Open standards and common design patterns

- *X.509 (PKI), X.509 PKI Profile, WSS X.509Token*: security token format, particularly for intra-organization use.
- *X.509 PMI, X.509 AC Profile*: potential uses include authorization tokens and enabling delegation of authority.
- *WS-Trust*: web service interface adopted for issuance and validation of security tokens, i.e., interaction between enforcement point and security token service; a specific profile is implemented.

- *WS-Federation, WS-Federation Active Requestor Profile*: the federation model is adopted; including configurable variants of identity providers and security session management services.
- *WSS SAMLToken, SAML Token Profile*: a custom token format is implemented for cross-organisation use; the SAML token format would be a good candidate to migrate to for the next version of the framework.
- *WS-Federation Passive Requestor Profile*: the eLearning scenario implements a custom username/password authentication scheme, but may likely adopt the WS-Federation passive requestor profile in the future.
- *SAML*: the SAML token format used for cross-organization use (see above); the SAML protocols are currently not adopted, as the WS-Trust protocols have been selected for token (including authorization tokens) interaction between enforcement points and security token services. Notably, the co-use of X509, SAML assertions and WS-Trust explored in TrustCoM is similar to the identity model being put forward for MS CardSpace.
- XACML is currently used as the main intermediate-level policy language for defining *attribute-based* Access Control policies that are loaded in an XACML compliant Policy Decision Point (PDP). Also XACML request / response operations in a SOAP envelope are used as a baseline for implementing message exchanges relating to access control policy decisions made by an XACML compliant PDP.
- *WS-PolicyAttachment, WS-MetadataExchange*: subject to resource availability, if the project timescales allow, we anticipate experimenting with these protocols for in-band policy exchange..
- XACML profile of SAML can provide an alternative protocol for interacting with XACML-compliant PDPs. SAML protocol is not considered at present as a baseline protocol for authorisation and access control request/response message exchanges.
- *XML Key Management (XKMS)*: as a VO-wide PKI was not a direct objective, this specification is not considered during the conceptual investigation.
- *Liberty, Shibboleth, Web Single Sign-On Interoperability Profile, Web Single Sign-On Metadata Exchange Protocol*: the project expects to assess interoperability with single sign-on systems.
- *Use of SAML for OGSA Authorisation Profile*: this is a relevant ongoing standards initiative, but a specification is not yet available.
- *WSS UsernameToken, WSS KerberosToken*: X.509 certificates are commonly used for intra-organisation communications; however the TrustCoM infrastructure can be easily configured to allow transparent use of these alternative token formats.

4.4.2 Project assessment

Work in this area is divided in the following four categories: (i) federation services, (ii) secure audit services, (iii) reputation services, and (iv) trust negotiation services.

Federation services:

In TrustCoM, our main achievement in the federation services area is the development of a partner-level security token service (STS) which provides security tokens to invoke web services in the scope of a particular VO.

The main challenges were to design an open and flexible solution that allows TrustCoM customers to customize the STS to their specific needs, and to enable customers to participate in a variety of different VO types. The result of our development is an STS that has a pluggable architecture and that provides a wide range of configuration options to the VO partner operating the STS. The default installation of the STS already contains a useful set of default implementations which have been developed for TrustCoM, so that the default installation can be used directly in the TrustCoM test beds. The customer operating the STS can also implement own customized modules for different claim types, for the actual STS business logic for a particular type of virtual organizations, for partner and membership management inside a VO, for the company-internal user management and for the company-internal resource-to-VO mapping.

In addition to these operational aspects of the STS, we developed a management interface to the STS which provides a customized management experience to the IT administrators and VO managers.

The last point to mention is the development of a set of profiles for SAML and WS-Trust; these profiles specify how SAML is used to represent security tokens in TrustCoM, and which information needs to be embedded into WS-Trust requests to request these security tokens and their validation.

Secure audit:

In this area, TrustCoM has produced a reference architecture and prototype of a SOA-based secure audit service (SAWS) that is exposed as a web service.

This is an asymmetric key based audit service. Previous audit services have been symmetric key based, which means that auditors, system administrators or anyone else cannot read or access the audit logs without going via the centralised audit service which holds the secret key. The central service is thus likely to be a bottleneck to performance. Using a SAWS private key to secure the audit logs means that anyone with access to the SAWS public key can independently validate the audit logs, and read the audit records (unless they have been confidentially encrypted by the audit record writer, which is allowed for in the design). This will aid auditors in their work.

Furthermore SAWS has been designed using a Trusted Platform Module (TPM) so as to improve the protection and trustworthiness of SAWS. Due to the current lack of a standard hardware TPM API, the current TPM implementation is software based and requires a predefined number of (N from M) administrators to unlock the private key of SAWS. Once a standard hardware TPM API becomes available, the current Java TPM software object can be replaced by hardware based TPM. Alternatively, hardware specific TPM modules can be written now to replace the software TPM.

The SAWS has been released as open source software under a BSD license for anyone to use, modify and enhance as they wish. This will maximise the benefit to commercial organisations. The main beneficiaries are any organisation that wishes to produce tamperproof trusted secure audit logs, either via a SAWS offered to a VO by a trusted third party, or for internal use by service providers.

Reputation management:

Work in this area focused on providing a recommendation-based reputation service that can be exposed as web service to multiple actors, i.e. requestors inspecting of a VO partner's reputation or clients offering recommendations that are incorporated in computing that reputation. The reputation service is configurable allowing any relevant actors to be internally modelled in the reputation service and allowing the use of different algorithms for calculating reputation.

So far, one basic algorithm has been implemented for demonstration purposes. This algorithm counts reputation as a real number in the (0 … 1) continuum implementing a simple recommendation and discounting algorithm where reputation values are commutative and associative, with each value having the same weight (so that opposite opinions cancel out).

Current work focuses on integrating a more comprehensive algorithm that is based on investigation of "best-practice" business engagement and performance assessment criteria. This algorithm is in effect a technical implementation resulting from knowledge transfer from research on socio-economic aspects and business engagement criteria, which has been carried out in the context of the workpackage focusing on socio-economic context of the project. We anticipate that this new algorithm will better reflect the ability of an actor to conform to its service level agreements.

The main beneficiaries of such a service are organisations that want to establish new business relationships (i.e. form a VO) with organisations that they have previously not had any interactions with. The reputation service can be offered as a capability offered to VOs by a trusted third party or as a local service that maintains the view of a single partner or a coalition of business partners about their potential collaborators.

Trust negotation:

In distributed environments parties unknown to each other are often required to establish mutual trust in order to exchange sensitive resources and to access to services. One approach towards

trust establishment on line between two parties is through bilateral and iterative disclosure of digital credentials proving properties of the parties. Currently, we have a trust negotiation web service supporting the operations to carry on a trust negotiation according to different negotiation strategies that allow to preserve the privacy of the two parties and to speed up the negotiation process.

The negotiation service provides three different operations, Start Negotiation, PolicyExchange and CredentialExchange. Start Negotiation allows setting the parameters necessary to carry on a trust negotiation. PolicyExchange allows a party to receive disclosure policies sent from the counterpart, evaluate them and generate a response message containing its own disclosure policies. CredentialExchange allows a party to verify the validity of the credentials received from the counterpart and to send to the counterpart a message containing its local credentials.

The trust negotiation web service has been developed in Java using the Tomcat Application Server and the Axis Soap Engine. The Oracle database version 10 g is adopted to store the disclosure policies and credentials necessary to carry on a trust negotiation. The trust negotiation web service supports two formats for credentials: X509 and a proprietary XML format. Also disclosure policies are represented in XML according to a proprietary format.

4.4.3 Recommendations

Further work for the remaining of the project in the area of federation services will focus on improving the modularity and configurability of security token services and on providing VO-wide security token services in order to facilitate VO Management and the management of security context that relates to a business activity executed within a VO.

Further work for the remaining of the project in the area of secure audit will focus on the integration the SAWS with the VO infrastructure and the SLA monitoring subsystems.

Further work for the remaining of the project in the area of reputation will focus, on the one hand, on the improvement of the reputation algorithms based on the experience from the research investigations in the contextual workpackages and on the other hand on integrating the reputation service with other subsystems by means of defining policies that can trigger adaptation in response to changes to the reputation of a business partner.

In the area of Trust negotiation, in the last phase of the project, we will work on the integration of the trust negotiation service with the VO Management toolkit. The trust negotiation service will be used to authenticate a member or an initiator when he registers to the host associated to a particular VO. At the end of the negotiation process the member/initiator send his public key certificate to the host. The host stores all public keys certificates of the members and may pass them later to the STS for verification.

4.4.3.1 Areas of further research and knowledge transfer

TrustCoM has made substantial progress towards realizing secure and manageable federation models that are based on open standards and are in line with the insights gained through project studies on business-to-business collaboration models and on legal issues underpinning Virtual Organisations. We anticipate that much of this work will find its way to enhancements of SOA-based middleware and commercial federation services. However, the advancements achieved within TrustCoM have created the possibility of conducting further research towards achieving more advanced technical goals in this area that are inline with the TrustCoM vision. One important area in this direction is the automation of VO life-cycle management through distributed transactions and the policy-based adaptation of the circle of trust underpinning a federation in response to contextual changes.

Another area is the investigation of credentials (including identity) brokerage and transformation schemes. Although our TrustCoM federation services are currently tackling the secure distribution and use of security credentials and identities, we have not been investigating or proposing schemes for representing, processing and translating such security credentials and identities. This is an area where semantic technologies may be able to provide effective solutions. It is recommended that the community supports further research on languages and models for representing credentials in the

context of dynamic Virtual Organizations, as well as, on techniques for transforming such credentials across trust realms.

Security enforcement and auditing are two areas where Trusted Computing Platform technology may play a significant role as an enabler of innovation. Although in the context of the project we will conduct preliminary research on this field, we strongly recommend that a further in-depth investigation is conducted outside of the scope of the project. Such an investigation will have to take into account the legal implications of using Trusted Computing Platform as one enabling technology that underpins ICT infrastructures for Virtual Organisations.

Finally further basic research is required in order to leverage the TrustCoM results that relate to the use of risk and business partner selection models and metrics for reputation systems, as well as the incorporation of reputation and trust values into the evaluation of service provision agreement and of adaptation policies.

4.5 Policy (access control, management and adaptation)

4.5.1 Detailed objectives and research challenges

Research challenges in the area of autonomic security management include the development of models and mechanisms that underpin the life-cycle management of federations of security realms of VO partners as well as security management within and across VO partner realms. Particular emphasis has to be placed on adaptation of security policy and mechanisms to changes in the VO context, self-management, and resiliency to faults or misbehaviour within the realm of a VO partner or the realm of its collaborators.

In order to tackle this extensive area more effectively and to identify common functionalities for policy management, delegation and adaptation. These may be of a more generic nature than specific to security; consequentlywe have decided to divide these research challenges into the following areas:

- Specific research challenges for "**access control policies**", including policies concerning the **delegation** of administrative authority. This includes the development of authorisation and delegation policy templates as well as the development of **Policy Decision Points** that have the intelligence to produce decisions at run time based on such policies.
- Specific research challenges relating to **adaptation**. These include the development of adaptation models, and notations for specifying policies that describing conditions under which the system may automatically adapt its behaviour and of services that implement adaptation actions, i.e. actions that result in adapting system behaviour in reaction to contextual changes.

It has to be noted that following the research conducted during the first half of the TrustCoM project in this area, it became apparent that a sufficiently generic form of adaptation policies underpins goals and/or solutions relating to other challenges such as VO management, SLA management and BP enactment. Consequently a set of goals relating to policies has been separated from the set of goals that are specific to trust, secure federation and reputation. The goals relating to the Policy address our specific research challenges relating to adaptation policies, on the one hand, and permission, prohibition, obligation and delegation policies on the other.

4.5.1.1 Emerging solutions relating to adaptive security and distributed access control

Security aspects of a VO framework span a large number of concerns that broadly divide in the following categories: Secure Federation, Authorisation, and Adaptive Security. In this section we focus on the latter two whereas section 4.4.1.1 focuses security tokens and federation. 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.

4.5.1.2 Open standards and common design patterns

- *SAML*: the SAML token format is currently used for cross-organization use (see above); the SAML protocols are currently not adopted, as the WS-Trust protocols have been selected for token (including authorization tokens) interaction between enforcement points and security token services.
- XACML is currently used as the main intermediate-level policy language for defining *attribute-based* Access Control policies that are loaded in an XACML compliant Policy Decision Point (PDP). Also XACML request / response operations in a SOAP envelope are used as a baseline for implementing message exchanges relating to access control policy decisions made by an XACML compliant PDP.
- XACML profile of SAML can provide an alternative protocol for interacting with XACML-compliant PDPs. SAML protocol is not considered at present as a baseline protocol for authorisation and access control request/response message exchanges.
- *Use of SAML for OGSA Authorisation Profile*: this is a relevant ongoing standards initiative, but a specification is not yet available.

4.5.2 Project progress assessment

So far, main achievements in the project can be categorised in two main areas: (i) SOA infrastructure services for policy management and adaptation (a.k.a. “Policy Service”) and (ii) SOA infrastructure services for distributed access control (a.k.a. “Policy Decision Point” - PDP). We review results in each area in turn.

4.5.2.1 Policy management and adaptation

The TrustCoM framework comprises a policy service which is able to enact adaptation policies in the form of Event-Condition-Action rules and thus to provide the means to specify declaratively:

- How the VO should react to events such SLA violations, loss of reputation, or intrusions at one of the partner’s sites. The ability to specify these rules in a declarative form permits to change the rules during the operation of the VO and also to adopt different rules in different VOs. The rules of a specific VO instance form part of the GVOA and are automatically enforced by the policy service.
- Which policies apply in given circumstances. Both adaptation and access control policies can be dynamically loaded and unloaded from the appropriate services without interrupting the VO’s functioning. Changes in the policy base can be specified as actions in adaptation policies thus enabling the VO to operate under different policies according to circumstances. Adaptation policies are thus a restricted form of programming of the VO and cater for a variety of VO requirements.
- How individual services must behave in response to VO events. The policy service can be embedded within other services in order to provide those services the ability to parameterise their behaviour using Event Condition Action rules.

The policy service realised as part of the TrustCoM project innovates over the State of the Art in several ways, including the following:

- It has an extensible architecture that scales from small devices to large servers. This is achieved by isolating core abstractions from application dependent code. Application and infrastructure

specific code can then be dynamically loaded according to the application needs. This makes the implementation suitable for pervasive systems and mobile-grid type applications as well as for traditional distributed systems and grid projects. An added benefit is that the service can be easily customized and embedded in other services.

- The policy service represents a web-service interface but can also use other communication protocols concurrently. This enables it to integrate with legacy applications as well as to interact with a wide variety of managed services and resources.
- The policy service can interact with multiple event systems in order to receive notifications that trigger policies. We have used the WS-Notification based service within TrustCoM but also have event adapters for XMLBlaster and other event service technologies.
- The policy service uses XML as a means of specifying policies but also as a means of sending commands to the policy service for a variety of other tasks.

Due to its flexibility and extensibility the policy service is applicable across a wide range of areas. It can be deployed in VOs in multiple ways and for a variety of tasks as discussed in [23]. It can also be used for network and distributed systems management and will be made available to the EU EMANICS network of excellence (http://www.emanics.org) as well as for security management and intrusion response. Due to its small footprint, the policy service can be used in embedded devices for autonomic management of pervasive systems. The main beneficiaries of the policy service itself are researchers in both academia and in industry working in these areas. However, as shown in TrustCoM, the policy-service can be used in conjunction with a larger framework that permits its deployment closer to market. We are in the process of publicly releasing the first version of the policy service as a stand-alone component but will also release it as part of the TrustCoM framework together with the code that ties it in the TrustCoM infrastructure.

4.5.2.2 Distributed access control and delegation

In the TrustCoM framework, the Policy Decision Point (PDP) implements authorisation and delegation policies, and responds to access control queries issued by the Policy Enforcement Point

Authorisation policies permit the specification and enforcement of access control rules that include constraints based on the attributes of the requestor and on additional context parameters such as time and the identities of the job and the VO in which the access request takes place.

At the core of our solution is a delegation mechanism that can be used to create authorisations both at the access level and at the administrative level. Delegation policies enable decentralised and distributed management of access control by making it possible to specify who may administer access control policies, based on the attributes of users, resources and administrators. Delegation policies are also useful in expressing the sharing of resources in a VO since such sharing entails delegation of access control. While a more decentralised administration of authorisations is necessary, it is equally important to maintain a degree of centralised control to prevent rights from propagating in an uncontrolled manner. The goal and the challenge of this research has been to develop a model for decentralised authorisation management, where the control of the propagation of rights is maintained, and even improved, compared with existing centralised authorisation administration models.

Besides offering an access request method to the PEP, the PDP presents an interface letting the Policy Service administer its policies. Although the TrustCoM framework favours web-service interfaces, these are easily replaceable by interfaces that use other communication protocols.

The policies developed in the context of the two test scenarios illustrate the power and flexibility of our approach by giving the local administrator of the service control over the effects of the policies that an external Policy Service may upload to the PDP.

The main beneficiaries of this effort will be large application developers, who can reduce development and maintenance costs by using a standardised, consolidated and centralised authorisation platform.

4.5.3 Recommendations for future research and development

For the remaining of the project work in the area of policy management and adaptation will be mainly divided into two categories:

- improving the integration with services in other subsystems and demonstrators, and
- provision of higher-level abstractions for interactions across policy services.

Although, the policy service is already integrated with a number of services within the framework such as the notification service, PEP, authorisation PDP and VO management, further work remains to be done towards improving the information flow and achieving integration with application services and within the testbeds and demonstrators. The effect of this further integration work is to enhance the spectrum of policy applicability and thus to permit an increasing part of the VO behaviour to be policy-driven. As explained in [23], multiple deployment scenarios are possible for policy services. Also as part of this integration work policy configurations for the specific VO instances have to be designed. The provision of higher-level abstractions for exchanges of policies across policy services would confer better support for more complex VOs and VO federation, but the latter is not in the critical path of the project.

The work accomplished within the TrustCoM project in the area of policy-based service management and adaptation takes a significant step towards the provision of policy-driven VO behaviour. Future work, outside of the scope of the TrustCoM project can focus on either bringing the software developed within TrustCoM closer to market or towards addressing fundamental research challenges that hinder the applicability of policies in more complex scenarios. Work that would bring the policy components closer to market includes enhancements to the usability and specification of policies including higher-level languages, graphical tools and integration with policy analysis components. Basic research work that would enable the applicability of policy based components in more complex scenarios includes research on automated verification of policies in policy exchanges, policy negotiation and integration of adaptation policies with constraint-solving and planning tools.

TrustCoM partners have been actively contributiing to ongoing standardisation efforts in the area of distributed access control and delegation. The PDP, as currently used within the TrustCoM framework, is based on the XACML 1.1 standard appropriately extended to handle delegation. During the last two years we have participated actively in the OASIS Technical Committee responsible for the XACML standard and we have already succeeded in carrying our delegation model into the forthcoming specification of XACML 3.0. In fact, our delegation model constitutes the main difference between versions 2.0 and 3.0 of the standard. In preparation for the next version of XACML, we have released an open-source implementation[3] of the XACML 3.0 draft that is currently being tested within the EU-funded Ambient Networks Project[4]. We plan to bring this implementation into the TrustCoM framework in the near future.

Follow-on work in the area of SOA-based components for distributed access control and delegation will address usability issues, like the definition and implementation of appropriate GUI interfaces to the PDP, the standardisation of these interfaces and the development of a set of best practices meant to guide users in most common usage situations. Performance optimisation is another important outstanding issue, as well as the security of the PDP, particularly with respect to Denial-of-Service attacks.

In a broader sense, the very dynamic nature of VOs calls for the research community to invest efforts in the development of context-based delegation and access control mechanisms. As a first contribution, these mechanisms would give support for dynamic attributes. Provided they can handle more general contexts, they will also facilitate the enforcement of authorisation and delegation within workflow systems.

---

[3] http://www.sics.se/spot/xacml_3_0.html

[4] http://www.ambient-networks.org/

4.6 VO infrastructure

4.6.1 Detailed objectives and research challenges

We have identified and clarified the need for an open standards-based common infrastructure that enables the secure and reliable exposure and integration of the services and resources offered within a Virtual Organisation. This infrastructure may be independent of the assets of the partners who may wish to form virtual organizations (independent in terms of the business function, of the ownership of its assets and of its operational management).

We have identified the following main research challenges in this area.

(i) separation of concerns between

a. the provision and management of business services by the business (in particular SMEs) that may like to participate in Virtual Organisations

b. the provision and operational management of hosting environments and supporting infrastructure services that enable the rapid deployment of application services by different VOs

(ii) developing business models and system designs that support businesses that would like to take advantage of a network-centric delivery model to reduce the opportunity-cost and the time-to-market for by:

a. *Maximising Return-on-Investment via outsourcing* the development of a dedicated dependable infrastructure and infrastructure services, the cost of which is often prohibiting for a single business that focuses on a vertical market.

b. *Alleviating the operational management cost* of service deployment and hosting by outsourcing hosting and operational management while maintaining overall control of the terms under which their business function is provided within Virtual Organisations.

c. Reducing the cost of building *a secure, reliable and accountable capability exposure infrastructure* by enabling the use of a purpose-built infrastructure capabilities for virtualising one's business functions as managed services.

d. *Reducing the risk of exposure to an open network* by leveraging on the experience of a dedicated infrastructure provider.

(iii) Optimising the time and effort spent for setting-up and dissolving Virtual Organisations and for implementing change during their operation.

4.6.1.1 Emerging solutions and trends

Our assessment indicated that although a relatively small, but rapidly growing number of research and commercial tools exists that claim to provide service deployment platforms or "glue" software for cross-enterprise integration, their maturation timescales are 3-5 years from now (i.e. 2008-2010) – anyhow none of these are targeting at supporting the life-cycle of dynamic Virtual Organisations, or are providing advanced security and SLA management features as yet.

Middleware in the first category (i.e. service deployment platforms) includes the Globus toolkit version 4[5] which stems out of technological innovation targeting scientific communities with an emphasis on resource hosting and integration. Such products are now evolving into being a

[5] Globus Toolkit v4 can be seen as a Web services based Grid middleware that facilitates the integration of services and resources that have been deployed on multiple hosting environments. See also http://www.globus.org

significant part of wider scope enterprise infrastructure systems such as IBM's Grid toolkit[6] and products from Platform Computing[7] and United Devices[8].

Software in the second category (i.e. "glue" middleware) includes emerging Service-Oriented Architecture (SOA) based Enterprise Service Bus (ESB)[9] products offered by small companies such as Cape Clear, Infravio, Blue Titan and Sonic Software. In this category, the products offered by Cape Clear and Sonic Software are representative. The Cape Clear ESB solution focuses mainly on the creation and hosting of standards based (Web) services. The Sonic Software ESB solution focuses more on offering managed capabilities message brokerage, reliable transactions, asynchronous messaging, etc.

In between these two categories lies a recent initiative by the Apache foundation to offer an open source ESB on top of the Apache Axis 2 platform. However this initiative was announced during the Summer of 2005 and it is still in an early incubator phase. Similarly to the above, this initiative aims at producing a general-purpose ESB and it does not aim at supporting of dynamic virtual organisations.

4.6.1.2 Open standards and common design patterns

In terms of common design patterns and open standards specifications, a number of specifications partly address some aspects of this objective. In particular:

- The SOAP and WSDL specifications offer a transport independent means for service-to-service interaction by exchanging meta-data (XML) based messages between applications that can be deployed upon different platforms and have been exposed as Web services.
- The WS-Addressing specification offers interoperable constructs that convey address-related information that is typically provided by transport protocols and messaging systems.
- The SOAP interceptor / Handler pattern offers a programming model for network intermediary network points to process message exchanges between services. These intermediary points may be deployed independently (a.k.a. "Interceptor") of, or co-deployed (a.k.a. "Handler") with a Web service endpoint.
- The WS Security stack of specifications is delivering a technical foundation for implementing security functions such as integrity and confidentiality in messages implementing higher-level Web services applications.
- The WS-Notification specification is offering a pattern-based approach to allow Web services to disseminate event related information to one other
- The WSRF/WSDM (or alternatively the competing WS-Transfer/WS-Enumeration/WS-Management) stack of specifications define a Web services architecture for managing distributed resources, including other Web services endpoints.
- The WS-Coordination / WS Transaction stack of specifications (and alternatively the competing WS-CAF) are defining an open framework for supporting coordinated transactional compositions of multiple Web service applications.
- *MTOM: Message Transmission Optimization Mechanism* SOAP Transmission Optimization Feature enables SOAP bindings to optimize the transmission and/or wire format of a SOAP

---

[6] See also http://www-1.ibm.com/grid/solutions/grid_toolbox.shtml?Open&ca=daw-prod-gridtoolbox

[7] See also http://www.platform.com/Products/

[8] See also http://www.ud.com/solutions/deploy/mp_enterprise.htm

[9] According to Gartner's definition, an ESB is standards-based middleware that uses a Service-Oriented Architecture (SOA) and that has messaging, intelligent routing, and transformation capabilities. In this document we follow other industry experts who validly extend Gardner's definition to include features like orchestration, security federation, and a common service management framework.

message by selectively encoding portions of the message, whilst still presenting an XML Infoset to the SOAP application. Permitting to binary files, run in a secure and protected environment.

Although the Web Services interoperability organisation (www.ws-i.org) has produced a basic interoperability profile and it is finalising a basic security profile, there is no current initiative to define profiles for realising the basic functionalities targeted by this research challenge.

4.6.2 Project self-assessment

Main achievements in the project so far can be categorised in two main areas: (i) messaging and policy enforcement and (ii) service virtualization.

Messaging and policy enforcement:

Work on enforcement and service management focused mainly on implementing a transparent and adaptive message interception and service exposure capability that used for exposing a (Web) service in the context of a specific VO. Service provisioning and exposure in a specific VO a potentially limited life-time that is tied to the period during which the service is offered in this VO, and which are "manageable" in the sense that their life-time and configuration can be set and changed programmatically by dedicated clients (e.g. administrator's GUI) or by management services.

The enforcement subsystem (also referred to as "Policy Enforcement Point (PEP) or "Messaging Service" – depending on which of its aspects is emphasised) exposes programmable interfaces that enable creating and configuring access points to the capability, based the context in which it is exposed (e.g. the VO and service provider). Managing the behaviour of the enforcement subsystem through programmable interfaces, allows interactions with different security and policy services (i.e. STS and PDP), depending on the context of the interaction. It also enables dynamic adaptation depending on actions on its management interface that are performed by the TrustCoM policy service. The latter dynamically evaluates event-based policies that trigger reconfiguration of the enforcement subsystem.

From a service client's perspective the enforcement subsystem exposes VO specific endpoints for a service and enables the service's availability in a VO. From a service provider's perspective, the enforcement subsystem enables to tailor the provision of the same business capability in the contexts of different VOs by enabling virtualization (i.e. creation of a distinct "virtual network endpoint" and a distinct "virtual identity" for a common capability) enforcing different policy, and integrating different federation, access control, SLA, etc., capability depending on the VO within which the service is being offered. From a VO manager's perspective the enforcement subsystem, facilitates interoperability and allows the monitoring and processing of all interactions and enables the dynamic adaptation to contextual changes.

One example of enforcement behaviour that has been paid particular attention is full blown end-to-end security enforcement[10] between two web services, as it provides the mechanism for fetching the appropriate token (including message encryption and/or signature) and authorising the outgoing message (at the originator side), and validating the token (including signature validation and/or message decryption) and authorising the incoming message (at the recipient side).

Service virtualization:

We use the term "service instance" to refer to the virtualization of a (Web) service for the purpose of implementing interactions within a VO. We call the (Web) service itself a "capability" in order to emphasise the fact that interactions with a VO take place only via a "virtual endpoint" dedicated to

[10] Successful completion of the enforcement assumes that: 1) the appropriate policy is retrieved form the resource property document, 2) tokens are successfully validated, 3) authorisation procedure conducted and results are used, 3) handler chain of a new instance is properly configured, 4) and the appropriate notification are generated and dispatched. In the case of a failure of an action (e.g. token/ signature validation, message part decryption, non-granted authorisation), the communication is terminated and the appropriate notifications are generated and dispatched.

this VO, i.e. through a VO-specific virtualization of the capability. Also the same capability has will have different "virtual identities" in different VOs. The Instantiation service is an advanced implementation of a commonly used creational "Factory method" design pattern[11]. It is usually associated with an already deployed capability that has been exposed as Web service. The Instantiator is exposed as a separate Web service and can create services instances of a capability at a service host. The main advantage of this approach is that it separates the deployment of a Web service from its exposure in a specific VO and enables the creation of multiple Endpoints, each of which comes with an explicitly described, security, contract and transaction configuration. Although the concept of a factory is well understood in CBSE and Grid Computing, the use of an Instantiation service for creating dedicated, manageable and reconfigurable service Endpoints is novel and offers a new perspective on what can be achieved by leveraging on the converging points of Grid and Web services technologies.

The Instantiation service provides the means by which one can request the creation of a new service instance for an already deployed capability. The instantiation implements distributed and asynchronous interactions that bring together a number of different VO infrastructure services in order to implement the process of creating a new service instance.

At present, this includes creating a new manageable endpoint, configuring the endpoint with the appropriate enforcement actions, and configuring all TrustCoM services that support the operation of the new virtualizations (i.e. "service instances") of an application service. Supporting services include the service provider's messaging service and security gateway (PEP), the provider's security token service (STS), the provider's access control decision point (PDP), the service provider's policy adaptation service, the service provider's SLA monitors, and audit services. Virtualization also includes configuring the bindings among the service instance and the supporting TrustCoM services. Finally, only if all the above steps are performed successfully, a reference to the endpoint of the new service instance is returned to the requestor.

4.6.3 Recommendations

One of the ongoing tasks is upgrading the PEP to support context-aware web services. In this direction we have focused on developing a coordination service which extends the basic WS-Coordination to include a set of context-bound tokens that secure the interaction between participating services. The work is in the final stage of prototyping, and in the current state comprises coordinator-driven interactions between a client (e.g. a web service) and context-STS that result in an exchange of a client's ID token for a context token. As a final stage of this task, PEP will be upgraded to allow automated separation of different PEP configurations (that protect different service instances), depending on the context of interactions – including the PEP obtaining coordination context and context-based tokens on behalf of the instance.

Regarding the service instantiation, next step is to integrate Instantiator with the VO management components, so that one can schedule instantiation of services based on the business processes defined in the VO, and configure these services using policies and agreements agreed upon on the VO level and kept in the various VO-level components.

What is also outstanding is to integrate SLA-related components (i.e. monitoring components, evaluators, SLA management services) in the instantiation process, so that exposure of service instances can be configured in accordance to the SLA – analogous to the way relevant policies are identified and activated. One of the main reasons for delaying this task has to do with dependencies on ongoing improvements of the SLA and Business Processing subsystems: activating an SLA instance requires that interacting entities are already identified, for which a VO-level business process description is required.

---

[11] See Gamma, E., Helm, R., Johnson, R., Vlissides, J., Design Patterns © 1995, Addison Wesley.

4.6.3.1 Areas of further research and knowledge transfer

Research challenges after the end of the project, that are subject to further research, knowledge transfer and advanced development include:

(a) The definition of widely agreed schemes for enforcement configuration policies in order to facilitate the interoperability between enforcement subsystems and management services, research in this direction is already described in [23]

(b) The definition and implementation of a management framework that enables the selective aggregation and efficient management of large numbers of enforcement components in an Open network; aggregation may happen sequentially, i.e. by intercepting or mediating in interactions between two services or in parallel, e.g. by aggregating components that have to protect services offered by the same provider to the same or different VOs. Efficiency in management means that common policy updates or life-cycle actions are instantaneously propagated over the network to a large number (e.g. hundreds or thousands of enforcement components and configurations).

(c) The optimal integration of a enforcement, service management, federation and policy management capabilities in a service gateway that enables the cost and time efficient virtualization and secure exposure of legacy applications in a VO over an open network. Although work in this direction has already started in TrustCoM (see [20] and [23] for example) as comprehensive architecture for such a gateway requires further research and experimentation

(d) The implementation of the above on clusters of hardware gateway devices such as those offered by IBM, Forum Systems, Layer 7 Technologies, Vordel or Reactivity in order to shift the resource intensive processing to specialised hardware.

(e) The enhancement of current Enterprise Service Bus products (such as those offered by IBM, Sonic Software, Iona, Infravio and Blue Titan) with enforcement, federation and policy management capabilities developed in TrustCoM in order to enable the use of mediation services for facilitating integration within Virtual Organisations.

(f) The development of automated analysis-techniques allowing to detect contradictions between global VO security policies and local policies of their partners, as well as the check that enforcement points (represented potentially in form of legacy code) actually “implement” high-level policies. Contradictious policies may result in blocking of transactions of the VO system which should in fact succeed.

4.7 Technology integration

Integration has been identified as one of the major risks during the first phase of the project. Following the decomposition of the overall research challenges into specific targets and decomposition of the TrustCoM framework into six subsystems (i.e. VO Management, BP Enactment & Orchestration, SLA management, Trust & Security Services, Policy & VO infrastructure). We had to allow the teams addressing subsystems the freedom to produce innovative designs in prototype implementations while maintaining a degree of consistency and convergence in order to alleviate the integration difficulties of interim results.

In order to achieve this, we took the following actions: Within the first part of the project, we created an internal representation where we maintain information about

- the main services (“capabilities”) provided in the context of each subsystem,
- the main interfaces these services expose,
- the main dependencies between services – especially dependencies across subsystems,
- and the main info-sets that characterise information specific to a subsystem or information shared across subsystems, including
  1. message exchange scheme,
  2. policy schemes, and

3. main transaction templates.

We also put in place a procedure whereby the organisations responsible for leading design and prototype implementation in each subsystem regularly update the information in the above representation and highlight changes that may have an impact in other subsystems. Major changes that affect dependencies can be implemented only if the directly affected parties endorse.

The following actions have been recommended [13] by the scientific coordination and technical management of the project for the second phase of the project in order to facilitate integration within the scope of the activities relating to the TrustCoM framework and its reference implementation:

1. The team working on the architecture revisits the designs of the services that have been developed so far and defines (in conjunction with the corresponding workpackages) basic transactions that span across the VO infrastructure and (trust, security, SLA) supporting services. Examples of such transactions include:
    a. Transactions that underpin the life-cycle management of service instances; this includes creating instances of policies that apply to the new instance and configuring the necessary policy decision points, identifying the necessary SLA and configuring the corresponding SLA monitoring and evaluation services in order to support the operation of a new instance or deactivate an operational service instance endpoint and implement the graceful destruction of that instance.
    b. Transactions that underpin reconfiguration or update of trust & security services (including enforcement, security token services, policy and reputation) in reaction to an SLA violation.
    c. Transactions that underpin adaptation to the change of the level of reputation of a VO partner or of the state of trust relationships between different VO partners.
    d. Transactions that underpin the life-cycle of secure federations across the trust realms of several VO partners.
    e. Transactions that underpin the distribution, enactment and adaptation of a collaborative process. Where adaptation comes in response to an SLA violation or a security failure.
    f. Transactions that underpin major changes to the life-cycle of a VO including formation, engagement of a new partner, disengagement of existing partner and dissolution.
2. The teams working on the different subsystems implement these transactions in a bottom-up fashion. This requires selectively integrating services on top of a common ICT infrastructure, implementing transactions for realising complex interactions between these services and adapting their interfaces where appropriate, and proceeding to the integration of a layer above once an adequate level of integration has been achieved at all levels below.
3. Identify selective integration that add value to each application scenario and try to apply them in the context of enhancing the corresponding application scenario testbed.
4. Understand the implications of the integration on the collection of open standards technologies used as a technological base-line in each case.
5. Understand the implications of the results of the legal and socio-economic research, and where appropriate, implement a selective take-up of these results in whenever they clearly add value;

Driven by these recommendations, in the second phase of the project we defined integration scenarios both in terms of the reference implementation and also in the context of the TrustCoM testbeds. Three integration scenarios have been defined (see also summaryin Figure 7):

1. The first integration scenario focuses on the formation (and dissolution) of a Virtual Organisation, including the completion of the General Virtual Organisation Agreement, the formation of the underpinning federation of trust realms and the virtualization of the services provided and assignment of the virtual identities to the users participating in a Virtual Organisation.
2. The second integration scenario focuses on the evolution of an operational virtual organization, including monitoring the agreements in place and adapting behaviour in

response to a contextual change such a violation of an agreement or a policy or deviations in the performance of a business partner (measured as “partner’s reputation”).

3. The third integration scenario focuses on the (normative) operation of a Virtual Organisation, including the execution of policies and transactions between consumers and services within a federation of trust realms that underpins an already established Virtual Organisaton. This includes enforcement of security policies and agreements, as well as the exchange and validation of credentials and the establishment, distribution and use of virtual identities.

The above integration scenarios have been further divided into phases that correspond to fulfilling subsets of more specific transactions that span across the subsystems of the TrustCoM infrastructure. See [20] for a more detailed description of the integration scenarios. Work on integration is currently ongoing and Integration is the outstanding challenge that has yet to be fully met by the TrustCoM consortium. Meeting these distinct integration milestones is a major outstanding research challenge for the TrustCoM consortium.

Another important issue relating to this area has to do with the availability and maintenance of the open source reference implementation of the project. Although it is the intention of the project to make this available to the public on the basis of open source licence agreements, it is imperative that the precise for of the license agreement for each collection of components is finalised before the end of the work on methods and tools, and that a means of ensuring widest possible availability and maintenance is identified. Different options such as availability via communal repository such as *sourceforge.net* or preferably the availability through another European initiative that focuses on open source SOA component repositories such as OMII or BEinGRID (www.beingrid.eu) need to be examined and pursued as needed. Obviously making TrustCoM components available via repositories such as the BEinGRID open source repository ensures continuity of maintenance and availability of the TrustCoM results.

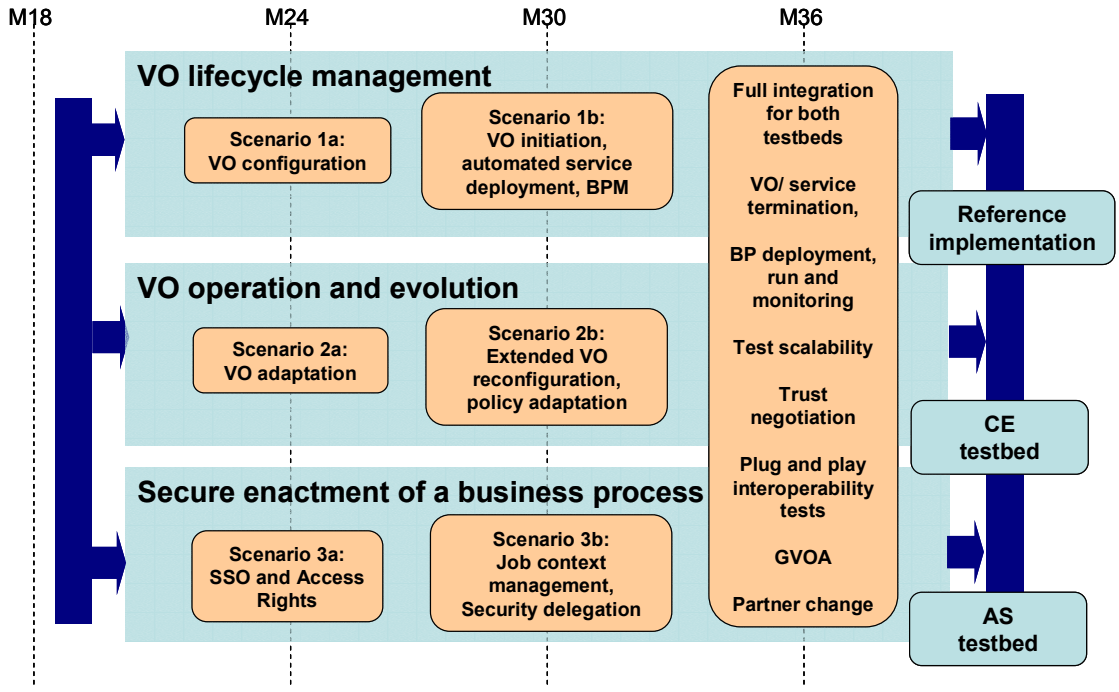


Figure 7: Overview of the TrustCoM integration scenarios and their planned phases

5 Progress assessment & recommendations: *contextual objectives*

In this section we first revisit our research objectives and challenges relating to the legal and socio-economic context and to work on technology standards, and then we provide an assessment of project progress and innovation in these areas. Work in these areas provides the business, legal and technology interoperability context that steers from different perspectives our work on the technical core of the TrustCoM framework. Legal and socio-economic research produces requirements and informs our conceptual models whereas work on standards informs our technology choices and facilitates interoperability and uptake of our results.

5.1 Legal Aspects

5.1.1 Detailed objectives

The objective of TrustCoM's legal activity has been to study selected legal issues in relation to trust, security and contract management for Virtual Organisations. Research focuses on the legal risks that may arise for VO members during the VO lifecycle. The work has been performed in close collaboration with other TrustCoM partners, in particular in relation to the TrustCoM application scenarios on collaborative engineering and e-learning. This work has contributed to the overall TrustCoM framework by defining legal requirements for trust, security and contract management.

The legal research performed by so far falls into three categories: *data protection law*, *intellectual property law* and *international issues*. Specific legal issues within these categories were selected based on their relevance for the TrustCoM project. The risk analysis results indicate how legal risks can be treated through an integrated solution that joins together contractual elements, trust management and security management. The contractual treatments should consist of an adaptation of a contract template to the specific risks identified in the scenario.

With respect to the Collaborative Engineering scenario, the legal risk analysis focused on *intellectual property rights* and *confidentiality*.

The legal analysis of the Aggregated Services / eLearning scenario focused initially on legal risks related to *international issues*, i.e. choice of law and jurisdiction and continued with a study of the legal management of *access rights*. The study aimed at providing legal requirements for the management of access to various learning contents during the provision of the E-learning courses in the AS Scenario.

In the last quarter the legal research focuses on identifying the risks to information that VO partners will have access to, with respect to

a. illicit access to confidential information by VO members or third parties, and
b. illicit dissemination of confidential information to entities that are not entitled to access the information.

With the aim of integrating the access based on policies as defined in the TrustCoM framework with the legal protection of confidential information, we discussed the legal protection of confidential information in selected statutory laws and assessed the need for additional contractual clauses specific to the application scenarios.

The main objective of the legal activity during the coming 6 months of the project will be to ensure the integration between the different monitoring instances created as part of the TrustCom architecture (i.e at a Trusted Third party level, as well as Service Provider domain and host level) with the legal requirements of the generation of monitoring data, notification and evidentiary issues so as to ensure not only technical viability but also legal compliance.

5.1.2 Key contributions and expected impact

Legal risk analysis allows the legal studies 'to have a proactive approach on legal issues, which can be seen as opposed the reactive perspective inherent in traditional legal methods. Moreover, legal risk analysis facilitates the integration of the perspectives of trust and security with the different levels of contracts for virtual organisations.

TrustCoM has followed an approach in which two classes of VO contracts are defined:

- *VO Contracts*: contracts that express the general rules that each partner of a VO must abide to. These general rules for of collaboration constitute the legal basis for the collaboration. They define how the VO collaborates towards the achievement of the common goal and how the partners jointly work with reducing the risks of collaboration.
- *Service level agreement (SLA)*: contracts that express the specific rules that partners involved in a specific (operational) business process must abide to, for instance Quality of Service (QoS) requirements for a specific service.

These contract types need to be related to the different organisational levels of collaboration. The creation of VOs may be facilitated by an Enterprise Network (EN), which is set up as a basis for more specific collaboration in VOs. This EN will and should also be based on a contract which should include rules about the collaboration at EN level and about the creation of VOs. Hence, if there is a contract-based EN, both VO contract and SLAs may be understood within the context of the EN contract.

EN contracts will be defined by the EN, based on the types of VOs envisaged by the network, taking into account the specific needs of the industry in question and based on the requirements laid down by the applicable national laws. Though templates and model contracts are available, it is not possible to draft one general EN contract for all domains. There will be major differences between possible networks in various industries, services, jurisdictions, etc. However, the more similar the VOs in the network are, the more details may be included in the EN contract.

A particular challenge in relation to VOs is the speed with which they may be expected to be formed, potentially on a time scale on the order of minutes or seconds. Creation and signing of VO contracts may thus need to be fully automatic. The drafting of some elements of the EN or VO contract will be based on the business plan and strategy, on the specific needs of the industry in question, and on specific requirements laid down by the applicable national laws. Moreover, the EN or VO contract needs to take into account risks related to the collaboration. This aspect can be covered in a legal risk analysis, which seeks to identify risks related to the collaboration, affecting either the common business goal or the assets of the participants.

To reduce the risks involved with establishing, joining and operating a VO, an approach for analysing and managing legal risks is needed which takes into account both technical and non-technical aspects. One of the goals of TrustCoM WP9 has been to develop methods and languages to facilitate legal risk analysis. These have been based on the existing CORAS model-based security risk analysis method and graphical threat modelling language. The updated risk analysis method, described in Appendix A, provides guidelines for identifying, prioritising and treating risks that can be addressed within an EN or VO contract. In addition, a simple checklist has been created for legal risks and treatments.

Risk analysis requires a clear understanding of the system or organisation to be analysed. The analysis typically involves a number of structured brainstorming sessions aimed at identifying and analysing risks and treatments. The effectiveness of such sessions depends on the extent to which the participants are able to communicate with and understand each other. We therefore propose the use of a graphical language for legal risk analysis, based on the CORAS graphical language for threat modelling. The language covers notions like asset, threat, risk and treatment, and supports communication among participants with different backgrounds through the definition of easy-to-understand symbols associated with the modelling elements of the language. Extensions for modelling legal issues have been made both to this graphical language and the Unified Modelling Language.

The work on legal risk management is expected to be taken up by lawyers as well as non-lawyers. There is already a growing interest for legal risk management internationally. Non-lawyers may use

the checklist, the contract model as well as the detailed legal studies on IPR issues, international issues and confidentiality issues in order to identify the most relevant legal issues for a secure collaboration in a virtual organisation. Lawyers and non-lawyers together may take up the methodology and tools for legal risk management, in order to carry out detailed analyses of legal and security risk aspects of information systems for virtual organisations.

5.1.3 Recommendations and outstanding research challenges

The main objective of the legal activity during the remaining of the project will be to ensure the integration between the legal requirements of the generation of monitoring data, notification and evidentiary issues with the information produced by the various monitoring components of the TrustCoM reference architecture and reference implementation during the operation of a VO that leverages on this infrastructure, so as to ensure not only technical viability but also legal compliance.

Future research will need to address a number of outstanding issues with respect to legal risk management. In particular, research will need to develop more specialized methodologies for legal risk management for other issues than those addressed here. Moreover, more research is needed regarding how exactly legal risk management can relate legal concepts like liability, enforcement, etc. with the concept of risk. Ultimately, the challenge will be to provide methods that can be used by non-lawyers in order to identify, analyse and address legal risks and non-legal risks in a timely and efficient manner, without the need for expensive

5.2 Socio-economic and business aspects

5.2.1 Detailed objectives

This work addresses the most fundamental questions related to business and socio-economic aspects of Trust and Reputation in Virtual Organization management. The technologies and standards based implementations for Trust and Security in VO frameworks provide a technical foundation for building secure advanced collaborative environments for business processes within and across multiple organizations. This work brings out the business, social and economics foundations for Trust and Reputation, with an emphasis on the following: a) Business Contracts; b) Business Metrics for monitoring performance driven by contract terms and c) Supplier Scoring and d) Business models for trust establishment.

Following a re-evaluation of the direction of socio-economic research during the first year of TrustCoM project (2004), the TrustCoM consortium set the following specific goals to drive research in this area, for the remaining of the project:

- Explore economic models of competition for Trust and Reputation in VO management and Industry supply-chains. This objective was to understand, expand or extend the competitive strategy driven models to include complex VO attributes for trust and reputation.
- Investigate and recommend Business models for VO management and VO supply chains and trust enablement through intermediaries, supply-chains and third-party entities. In particular focus on CE scenario in TrustCom.
- Investigate Trust and Reputation models for VO lifecycle management using models of business contracts and business metrics between VO members. The contracts include one-to-one and one-to-many configurations.
- Provide analysis and best practices from Industry Supply-chain models for Trust and Reputation in VO management with specific emphasis on the CE and AS scenarios.
- Provide recommendations and runtime system design for Member/Supplier scoring and Reputation for VO management, SLA management and SLA enforcement.

5.2.2 Project assessment

During the first seven months of the project in 2004, competitive game models were applied for VO selection and trust enablement between two parties. The models developed were focussed on individual trust models and not entirely suited to the requirements of the complex VO lifecycle management, which involves complex relationships between the VO members (group level network level trust). The game model was applied on a few attributes of the members and deeper insights into VO management were not revealed. Based on the reviews done in April, 2005 the objectives were modified during November, 2005 towards models of Reputation, Member scoring methods, industry best-practices in supply-chains, Business models for Trust and others. The final modified objectives are as follows:

- Investigate and apply advanced multi-tier Models of Business Contracts and metrics for VO Management, and contribute the models to AL1 and AL2 (action lines).
- Investigate Business Models for Trust and Interoperability between VO members and other VO organizations. Explore third-party neutral or dominant group environments for VO management and CE scenarios (Design engineering scenario).
- Investigate and apply Business Contracts and corresponding Terms and Conditions from industry supply-chains to VO Trust, member selection and reputation. Contribute to AL1 and AL2 activities.
- Investigate models for Reputation based on metrics defined around contract terms and conditions. Investigate advanced scoring models based on Industry practices in supplier selection using multiple criteria (for new and existing supplier selection).
- Provide recommendations on contract models, business models, reputation methods, member selection and scoring to actions lines in TrustCom (AL1 and AL2).

5.2.2.1 Interactions and impact on the rest of the project

We have taken several actions throughout the project to ensure integration and knowledge transfer between the socio-economic activities and the technical core of the project. Indicative interactions include the following:

- Work closely with the teams working on the technical core areas in order to jointly address issues on Business Contracts, Terms and Conditions, VO management and Business Metrics for Reputation and VO supply-chain models.
- Work on Business Contracts has contributed industry content and criteria to the core technical activities. Currently a working group has been established between multiple partners (spanning across all technical core and contextual activities) in order to investigate the role of Business Contracts in VO supply chains, VO and SLA management and in designing reputation mechanisms. WP8 intends to provide advanced knowledge, definitions and mechanisms around Business contracts to SLA and VO management.
- Technical input has been provided from the socioeconomic activity to to the “Generic Reputation Service” (section 4.3) which is an important part of the VO lifecycle management and Trust/Security Services. The input has been on Scoring methods, supply-chain metrics, contract based attributes and management for building an industry oriented reputation system.
- Technical input and steering of development or reputation scoring has also provided input to VO management (section 4.1), reputation models and scoring functions for VO members in a VO environment.
- Continuous interaction with TrustCoM standards related activities including initiatives on standards for business contracts, and models for interoperability between cluster of projects in the eGovernment and eBusiness area.

5.2.2.2 Key contributions and impact on the rest of the project

Results of this work describe in depth business models, contracts and supplier (or member) selection methods for VO (Virtual Organization) collaboration, interaction and sharing between

businesses in order to provide better transaction efficiency and better profitability. Research in this area investigates the assertion that business contracts with appropriate business models and member selection provide necessary foundations for enabling trust and reputation between businesses in a VO environment. In [21] we also illustrate the importance of supplier (member) scoring and rating from practices in industry supply-chains, and how they can be applied for effective VO lifecycle management. An overview of the relevance and impact of the results of this research to the rest of the project is provided in the following figure:

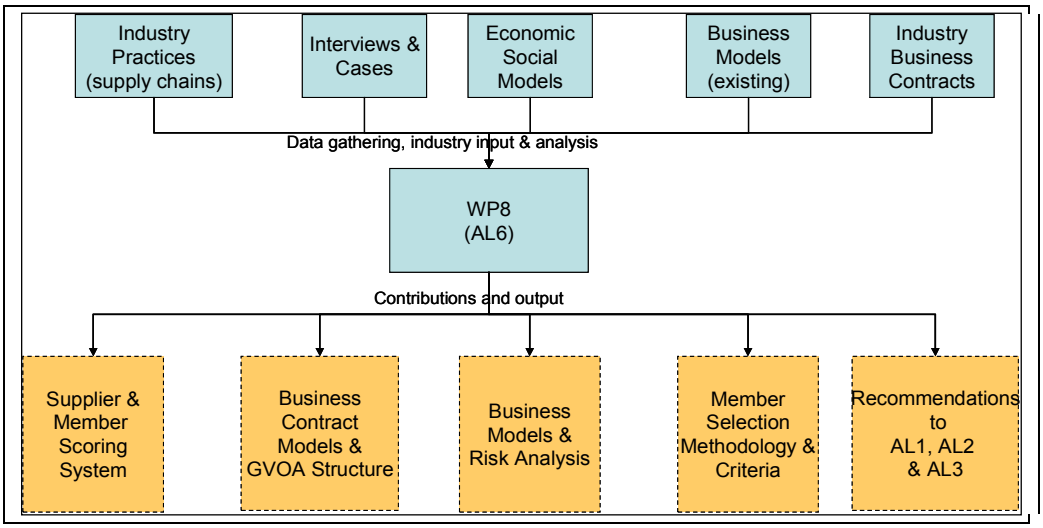


Figure 8: Contributions of socioeconomic context and business models to the TrustCoM framework

Other, more specific, contributions of the research in socioeconomic aspects and business models include the following:

- Developed a model of Business contracts for enabling VO supply chain interactions based on terms and conditions between VO supply chain partners. This is described in section 2 of this document in great detail.
- Developed novel reputation structures based on industry supplier criteria, business contracts and contract-specific terms and conditions. In this document we refer to VO members as suppliers (and we interchange the terms often). In most cases the VO manager is trying to form a consortium of members (suppliers) for specific applications. The reputation model is based on monitoring contract terms and conditions over a long-period of time in order to score and rate VO members. Business rules can be set by the VO members on the violations to select the VO members.
- Industry driven models for scoring based on contract attributes and functions for VO member reputation. The attributes for reputation are based on rules applied to the terms and conditions. If multiple terms and conditions are violated the scoring function considers multiple attributes and weighting functions based on the semantics and criticality of the violations.
- Business models for Interoperability were developed as a part of [14]. The models for interoperability considered trusted third-party, trusted consortia and trusted group models. The models apply to CE and AS scenarios and the VO management scenarios.
- Conducted industry research into the role and application of reputation. Used this research to drive reputation models and contracts.
- Industry-based model and methodology for risk and criticality assessment, which can be applied to TrustCom Business models. Identified levels of criticality and risk tolerance to drive the criteria for supplier selection process, scoring, and management.

- Contributed to models, process, and methodology for supplier selection based on industry research and standards. The contribution of models also includes supplier selection criteria at three levels of granularity: supplier, process, and product. The methodology has been applied to the TrustCoM business models.

5.2.3 Recommendations

The major conclusions and contributions of this work are as follows (see also [21]).

- Economic models play a strong role in enabling trust mechanisms. The document describes the various business models for enabling trust in third-party environments. The models were compared and contrasted based on risk, cost and other factors. The major result is that trust between parties or players is better with more history of transactions, metrics and assurances.
- Contracts are the life-line of building trust in Business Environments and VO supply chains systems. Design of contract structure based on industry knowledge for multiple service providers was the main contribution. The business terms and conditions in the contract and the contract content are the additional contributions.
- Business Metrics based on contract terms and conditions are critical for evaluating the reputation of VO members, monitoring the contracts terms and ensuring the proper enforcement of the terms. The metrics are captured and provide input to generic reputation system models for rating and scoring VO members/suppliers (see also “reputation service” in section 4.4).
- Criticality and risk are required precursors to the supplier and partner selection process. Criticality and risk assessment models were developed for the purposes of measurement and communication of these values for TrustCoM VO members.
- The supplier selection process consists of six basic steps including the analysis of risk and criticality. A methodology to support this process has been developed with supporting tools that can be employed in a manual or automated fashion.
- Risk manifests itself differently in the various CE Business Models. The same models also apply to AS scenarios. Opportunities to pool and transfer risk in partnerships and consortia were identified. The supplier selection methodology is consistent across the CE Business Models.

Products and services present unique characteristics; however, common criticality, risk, supplier selection, and management methodologies are applicable. Differences in product and service sourcing decision are reflected in the supplier selection criteria that have been developed and would be further developed through the presented methodologies.

5.3 Open Standards

Standards are a way to promote and achieve interoperability between technologies across different vendors. While businesses need to balance between agreed functionality, competitive advantage, and need for interoperability, interoperability is a key requirement in today’s multi-vendor market. Standardisation is an important part of successful exploitation. TrustCoM therefore aims at building upon existing well established and accepted standards and published specifications, where appropriate. If new technology is not compatible with existing standards that are well established in the market, then it may be more difficult to commercialize this into products and services which can interact with products and services provided by others. TrustCoM furthermore intends to contribute to the evolution of, and feed research results into, standards, where and in which way appropriate. The TrustCoM Standardisation Roadmap supports and documents the standardisation activities within the TrustCoM project, and is regularly updated throughout the lifetime of the project.

The first version of the TrustCoM Standardisation Roadmap [3] established a first baseline for further standardisation activities, identified the standardisation areas which are relevant to the project, and provided an initial assessment of the state of standardisation in each of these areas.

Subsequent versions [15] and [19] give a precise positioning status for each relevant standard and published specification, with respect to the first implemented version of the TrustCoM framework. While the list of standards and specifications relevant to TrustCoM has been growing during the last months, we have at the same time positioned the relevance of each of these specs in a fine-grained, qualitative way. Within each of the TrustCoM subsystems this had led to a clear identification of standards and specifications that have been adopted in the first version of the framework (as such, with restrictions, or adapted), standards and specifications that will not be considered, and standards and specifications that have appeared more recently and are kept within the relevance horizon for further investigation if time permits. This information intends to serve two purposes:

1. We provide feedback to the standards world on the applicability of existing specifications within the TrustCoM framework and on the effective impact of standards on the different subsystems in TrustCoM.
2. We inform the outside world of the standards choices made so far, in order to get feedback and to promote interoperability with products and services as well as research work in other projects.

As a pre-requisite for any standards adoption or contribution, the TrustCoM standardisation activity further analyzed the TrustCoM framework subsystems in order to get a more concrete picture of the different artefacts in the TrustCoM framework subsystems, particularly where these are relevant to interoperability. This activity further stimulated the conceptual work as well as the ongoing software developments to explicitly take into account interoperability requirements and to define clear and concrete specifications, which can be validated in the integration scenarios.

5.3.1 Adoption of existing standards and specifications

TrustCoM aims at building upon existing well established and accepted standards and published specifications, where appropriate. Particularly within the baseline infrastructure, TrustCoM has made a good choice in adopting various WS-* standards and specifications.

At this point there are still multiple, alternative web services specifications suites (i.e., WSRF/WSDM vs. WS-Transfer/WS-Management, and WS-Notification vs. WS-Eventing). For short-term prototyping reasons, TrustCoM has opted for the use of WSRF/WSDM and WS-Notification in selected cases. Within the context of the TrustCoM framework, there are however no fundamental reasons to adopt one or another. Specific profiles are moreover defined to allow easy migration from one to the other. This fits very well together with the recent commitment from the industry to define new specifications and enhancements which will enable further convergence of the different platforms.

5.3.2 Profiles

The primary focus of the TrustCoM standards and collaboration activity is in the creation of profiles that integrate existing standards *across* the different areas. While there are already numerous specifications addressing various issues *within* most of the identified areas, there are almost no concrete guidelines at all with respect to combining different specifications into a single interoperable framework.

The following concrete profiles have been and/or are being developed:

- A WSRF ResourceProperties document is specified that holds trust/security, SLA, and configuration policy information for a virtualized service, (possibly) including application state, and all this in relation to a context. This is accompanied with a profile for a service management service exposed as a WSRF enabled web service that contains a single resource property document per virtualized service. The restriction to a single RP allows easy migration to WS-Transfer.
- Related to this, TrustCoM has the expectation to produce specific design patterns for web services, particularly addressing instantiation and factory of web services.

- A security profile for WS-CDL is being developed that allows stating of BP description relevant security requirements.
- A profile that captures all SLA relevant structures is being developed. This profile is strongly influenced by both WS-Agreement and WSLA specifications. Interest from the WS-Agreement working group is being attracted.
- A profile for WS-Trust and SAML assertions for scoped federations is defined. This profile mainly covers specifications within the security domain, and addresses some cross-issues with Policy (XACML).
- A profile for using XACML in a VO context is defined. As highlighted below, SICS is contributing to future versions of the SAML profile for XACML being a member of the OASIS XACML TC.
- Profiles around coordination are being developed, particularly combining WS-Coordination with WS-Context, and including the use of WS-Trust security token services and XACML policies for issuing and validating such WS-Context based context tokens. TrustCoM is also looking further into coordinator interposition for federation bootstrapping. There is a high probability of defining atomic transaction types for EN/VO configuration processes.
- We identified the requirement for a profile for signing documents in a VO context. This is currently needed for signing SLA as well as policies within a VO.

The different subsystems are ultimately integrated through the General VO Agreement (GVOA) which is the central place for defining, linking, and agreeing specific terms that are relevant in the various subsystems.

The work in the application scenarios does not only validate the above profiles with respect to addressing the security, contract, and business processing requirements, but also provides useful experience in how the TrustCoM framework can be integrated into application services. For example, the current approach for service management does not mandate application services to be aware of the collaboration scope within which they participate, if this is not part of their business logic.

5.3.3 Specific new contributions

Where appropriate, TrustCoM may propose new contributions, based on its framework specifications. These new contributions may be introduced as new standards, or, preferably, as extensions on top of existing standards. For new contributions, we want to adhere to the principle of composability, and want to avoid unnecessary expansion of existing specifications.

In addition to various extensions which are part of the profiles listed above, the following separate extensions are defined in the TrustCoM framework:

- An extension of the UDDI BusinessEntity element for VO Member description is defined. TrustCoM is also considering the use of UDDI Categorization to define additional attributes on VO members.
- SICS is contributing to future versions of the SAML profile for XACML, which would be more suitable for delegated use. In particular, XACML 3.0 will contain the delegation functions used in TrustCoM in native and more clean form.

Besides these extensions, a number of TrustCoM proprietary specifications are developed for specific functionalities needing interoperability, typically within a single subsystem.

5.3.4 Dissemination within standardisation initiatives

A substantial part of the standardisation activities consists of disseminating and discussing (intermediate) TrustCoM results within standardisation initiatives, and within the individual partner organisations, with the people who are active in the existing standardisation efforts.

The following activities must be highlighted:

- HLRS and SICS are realising a profile that captures all SLA relevant structures, with a strong influence of both WS-Agreement and WSLA specifications. Interest from the WS-Agreement working group is being attracted.
- SICS is contributing to future versions of the SAML profile for XACML, which would be more suitable for delegated use. Erik Rissanen is a member of the XACML TC and is participating in the discussions. The plan is to continue to learn from the TrustCoM experience and bring in the results into the TC work at an appropriate time. In this way the relevant TrustCoM results could eventually be moved into the standard. Specific TrustCoM requirements to address in the XACML TC is the need for signing with security tokens other than X.509 certificates, and the expansion of the PDP interface with methods for loading signed policies. In particular, XACML 3.0 will contain the delegation functions used in TrustCoM in native and more clean form.
- SAP is promoting TrustCoM's top-down approach for VOs in collaborative business processing with relevant organizations, and has particularly brought up specific issues arising with the currently favoured bottom-up approach.
- UoK is co-chairing the GGF OGSA-Authz WG, and relevant trust, security, and policy TrustCoM work is influencing the specifications that are being developed in this working group.
- EMIC is disseminating the WS-Trust and SAML assertion profile to the relevant people inside Microsoft Corporation.
- BT promotes and aligns TrustCoM work with corporate internal web services initiatives as well as feedback to standardisation bodies, where BT is represented, including W3C (focusing WS Core and on WS-Addressing) and OASIS (focusing on security and web services management) and interoperability work within WS-I.
- CCLRC promotes TrustCoM work, particularly around GVOA, within the CCLRC E-Science Centre, expecting this work can be leveraged and integrated into other projects.
- IBM is investigating ways for TrustCoM to influence WS-Agreement based on the Industry Business Contracts, GVOA and SLA work that is currently underway in AL6/AL1/AL2.

6 Business demonstration areas

In this section we conclude the self-assessment presented in this deliverable by underlining the value of the business pilots (viz TrustCoM demonstrators) that have been selected for proving the business viability of selected results of the project, which are judged to be nearer to commercial exploitation and uptake. We summarise the motivation and scope of each demonstrator, the key stakeholders involved and the main success criteria we have set to the project in this important area.

6.1 Aggregated services

The Ad Hoc Aggregated Services (AS) demonstrator will be a prototype environment supporting ad hoc integration of services within loosely-coupled business communities (a Virtual Hosting Environment), built according to the principles of TrustCoM Framework.

The Virtual Hosting Environment (VHE) is an important concept to emerge from TrustCoM. It is an implementation of the kernel of the TrustCoM framework operated by a hosting service provider as the nucleus around which communities of enterprises may form. We expect that the Virtual Hosting Environment concept will be widely taken up. It offers substantial business opportunities to service providers, especially existing operators of telecommunications networks, data centres and application hosting facilities. The existence of VHE implementations will create opportunities for companies and other organisations to form Enterprise Networks[12] (ENs) and other communities on a commercial or public service basis. In turn, the availability of these safe environments for co-operation will remove barriers to the blossoming of an ecosystem of innovative small companies and be a considerable stimulus to European economic prosperity.

The primary target market is loosely coupled communities of SMEs operating in a given market sector (e.g. eLearning). Other related markets are health service provision and local community services. It is possible, however that large corporations would also see advantages in a third part service facilitating secure and easily managed business process integration.

A typical SME-based scenario would be the following: A VHE operator (say BT) offers a ('virtual') hosting service to SME enterprise networks, i.e. it provides a platform hosting kernel services to which the participating SMEs federate their resources. A customer organisation approaches BT with a view of establishing an SME EN in a particular business domain (eLearning, say). The EN is 'instantiated' with an initial core membership (maybe just the founder) and opened for business. SMEs approach the EN management to join the EN. The joining process involves various things like federating the new SME's platforms with the EN core platform, agreeing to contracts, registering services, and so on. A customer comes along with a particular requirement, and a set of partners and services are selected from within the EN community, etc. The VO is formed and interacts with the customer to agree and deliver services.

There are three main business roles in this scenario: VHE operator, EN founder / intiator, EN member, plus the end-user / customer role. The business models for players of the business roles are as follows:

[12] Within TrustCoM we are using the term Enterprise Network (EN) to refer to a community of companies – typically operating in a particular industry or application domain - that is bound by agreements, conventions and procedures that facilitate the formation and operation of Virtual Organisations (VOs) by the EN members. Thus, the VHE supports two levels of community: the EN, being an ‘ecosystem’ of entities willing and able to form VOs, and the VOs themselves, many instances of which may co-exist within an EN.

Business role	Business advantage of VHE
VHE operator the entity hosting the enterprise network and providing re-usable infrastructure and core services	This is a new business role, though related to application and datacentre hosting. For a NGN operator such as BT, it is an opportunity to leverage existing network infrastructure to provide added value, higher margin services.
EN founder (or initiator) the entity running the EN. It may also be a service provider/consumer within the EN. It is similar to the VO initiator in other TrustCoM scenarios.	This is assumed to be an entrepreneurial entity or one motivated by a wish to serve or promote the formation of a co-operating community. It may also be an EN member. It would have problem domain knowledge or business expertise as its core skill. Existence of a VHE would enable it to launch and operate an EN with little capital investment and relatively little technical expertise.
EN member a service provider and/or consumer within the EN community	The VHE concept allows the EN members to outsource the support for co-operation. It decreases the need for capital investment and specialist and lowers the barriers to short-term co-operation with occasional business partners. In addition, integration of the VHE platform with an underlying 'capability-oriented' NGN infrastructure would allow member services to draw upon a wide range of network-based services (e.g. billing platforms).

The main objectives of the demonstrator are::

- To make progress towards commercial exploitation of TrustCoM framework.
- To create a pilot VHE, i.e. a platform based on the TrustCoM framework that a provider (e.g. BT) can use to offer services to VOs.
- To evaluate the potential for integration with 'capabilities' exposed by IP-based Next Generation Networks (NGNs), e.g. BT's 21st Century Network (21CN).
- To show commercial potential via a convincing example application. The one selected is set in the eLearning sector.

The ultimate criterion for success is take-up by a network operator or another service provider of the TrustCoM framework realised in the form of a VHE. This is unlikely to be seen before the end of TrustCoM, but the likelihood of this happening will be assessed by gathering feedback from TrustCoM partner lines of business, advisory board members and external bodies.

There is a high degree of synergy between the VHE concept and the move to a service oriented approach to exposing generic network 'capabilities' taken by some network operators, and we expect the idea to be taken up readily. The existence of a third party services facilitating agile cross-enterprise integration will stimulate European business innovation by enabling small and start-up businesses to compete through co-operation. The potential for highly beneficial impact for Europe is therefore strong.

6.2 Collaborative engineering

The demonstrator is intended to show how TrustCoM can provide manageable security and assured QoS to collaborative engineering projects, and specifically simulation using engineering-strength applications and data. The primary objective is to demonstrate secure collaborative business process execution along with effective service performance monitoring. A secondary objective to show how service suppliers can be managed within an automated management framework based on a Virtual Organisation model. The business prototype includes application services hosted by BAE, Atos, HLRS that are extensions of the work that has been done in AL2. BAE will play the role of a mock business client in the application scenario and a number of supporting TrustCoM services will be provided by other project partners acting as 'supporting service providers'.

There are two main external business drivers that have influenced the demonstrator. The first arises from the need to increase the tempo of the design cycle in order to investigate new ideas for products while identifying and alleviating possible risks of sharing capabilities between JV partners, University Research teams and software engineering houses. The second driver is the need to improve supply chain performance by integrating services provided by external suppliers, software houses and internal IT systems within business applications. These internal business applications would produce an enhanced capability that potentially improves the performance and visibility of the component ordering process. The important factors in both cases are security and a flexible infrastructure that enables the rapid definition and enactment of a business process between organisations. The CE Demonstrator focuses on the design phase of the lifecycle and therefore has closer associations with the first business driver, though the implications for the second should be clear as well.

A key assumption of the business scenario is that Engineering application software can be made available as application services using web services technology, making them quicker to deploy into clients' processes and applications. The challenge for the TrustCoM Reference Implementation is to provide management infrastructure such that service clients are confident that the services they access from a market of service providers are secure, reliable and bound by agreements that can be monitored by systems. Manageability becomes another concern from both the client and provider perspectives as services become ubiquitous and integrated into products and applications.

The targeted markets include:

- Engineering companies who are involved in collaborative projects and wish to share in-house design applications as services in order to provide rapid support for novel products,
- Engineering software houses who provide specialist software, especially those applications that require HPC facilities,
- Providers of HPC computing, whose business model involves providing specialised computing resources to the widest possible number of clients with minimal administration costs, and
- Customers who wish to minimise internal IT administration costs and outsource eg, HPC computing resources, to external providers and who wish to have mechanisms for security and QoS.

The key stakeholders include:

- Design teams wishing to share applications with JV partners and to be able to access novel capabilities from University research teams,
- Software houses who wish to deploy their applications as services within an open business network,
- University research teams who wish to share novel technologies within pilot, proof-of-concept studies with industrial partners,
- Business policy makers and decision makers who wish to create collaborations through sharing of information and applications between organisations, and
- System administrators who wish to simplify the management of services.

The success criteria for the CE Demonstrator include:

- A demonstration that non-trivial engineering applications can be deployed as services and integrated within the TrustCoM framework,
- A demonstration of flexible, federated security between organisations, enabling a collaborator to access, eg, a design document provided by another collaborator,
- A demonstration of how a document binding the consortium- the GVOA- can be quickly composed and then expressed as machine understandable policies, and

- A demonstration of how the TrustCoM process management sub-system allows the collaboration to seamlessly deal with poorly performing suppliers and replace them with alternative service providers.

The expected impact includes among others:

- In the near term, the federated security model is of particular interest. This would help in the integration of applications from different security domains across the company,
- In the medium term, when the outsourcing of critical services to external providers has been achieved and security concerns are answered, systems for managing and monitoring SLA will be crucial for maintaining and improving business performance, and
- The overall long term impact of the whole integrated framework is in the automation of service provider management. This critically depends on the success of the first two aforementioned phases.

7 Conclusion

An interim progress assessment conducted by the project's scientific coordination and management teams during the first year of the TrustCoM project [13] identified as a major risk that the consortium could spend an unreasonably large effort into analysing dependencies between the various aspects of the TrustCoM framework at the expense of producing interim results in any of these areas. Consequently it was recommended that the project structure is drastically changed in order to achieve a clear separation of concern between the main aspects of the TrustCoM Framework and focus on producing a first round of tangible results in each area. In turn this brought about a major project restructuring that has been unprecedented for a collaborative project, especially if one takes into account that this restructuring was implemented following an internal project initiative and not an external review.

The restructuring of the project plan and re-focusing of work in specific self-coherent sub-areas has been successful to the extent that the newly formed teams focused on delivery within their respective areas of expertise Within tight timescales, the Consortium produced substantial advancements to the state of the art, and in many cases we managed to place ourselves ahead of our contemporary research trends.

In particular, TrustCoM has produced a collection of SOA based capabilities, implemented using "next generation" Web services technologies that enable:

- The life-cycle management of federations and Virtual Organisations.
- The secure exposure of applications as virtualized Web services that are tailored to the policies and agreements governing a Virtual Organisation.
- The declaration and use of General Virtual Organisation Agreements that amalgamate business and technical agreements which govern the operation and evolution of a Virtual Organisation.
- The federation of autonomous administrative and security domains (i.e. "trust realms) in order to support serve-service interactions in accordance to VO wide policies and agreements.
- The management, exchange and transformation of security and policy attributes in such federations, including the distribution and management of virtual identities,
- The management, binding and monitoring of service level agreements between consumers and providers of services in a Virtual Organisation.
- The deployment and execution of distributed processes using the most appropriate methods at different levels of granularity, i.e. choreographing processes across different partners in a Virtual Organisation while orchestrating services within each partner in order to fulfil a VO partner's segment of the choreographed distributed process.
- The enforcement of VO specific policies via a flexible SOA-based infrastructure that is independent and complementary to the business logic of the application services offered within a Virtual Organisation.
- The policy-driven adaptation of the SOA-based infrastructure in response to contextual changes during the operation of the Virtual Organisation.
- The provision of optional added value services for monitoring, reputation management and auditing based on patterns that have been derived by analysing business partner selection criteria in the selected application domains.

The design and development approach followed throughout the project leverages on SOA principles and Open standards based Web services technology in order to ensure that services fulfilling each of the above capabilities can be exploited either as a part of a reference implementation that realises the reference architecture of the TrustCoM framework or as independent capabilities in different contexts, therefore maximising the exploitation potential and potential impact of the project results.

These technical results have been informed and steered by more foundational research in legal and socio-economic aspects including both the legal issues that arise by the use of the technology in a business to business context and the incorporation of well established business practices about supplier-consumer relationship management and business partner evaluation and selection criteria.

During the second phase of the project substantial effort has also been made towards integrating the results instead of falling victims of our early successes by focusing on perfecting our partial solutions. For one of our main objectives – one that is particularly difficult to classify in any specific research area and has been a major motivation for bringing this Consortium together – is to produce a comprehensive framework in order to overcome shortcomings of previous attempts which fail at the boarders of the self-coherent albeit partial solutions they offer. In addition to improving the solutions in each set of capabilities, the TrustCoM consortium defined integration scenarios that focused on the different phases of the VO life cycle (formation / dissolution, evolution and operation), which complement the project testbeds in maintaining cohesion across the TrustCoM subsystems, application scenarios and contextual research.

Work on integration is still ongoing at this stage. Notwithstanding the specific recommendations and targets set for the continuation of research and development in each aspect of the TrustCoM Framework, meeting the above integration milestones is a major outstanding research challenge for the TrustCoM consortium. A very important issue related to this aspect has to do with the ensuring the availability of TrustCoM reference implementation as open source after the end of the project. One option to consider includes making the TrustCoM reference implementation available through open source repositories maintained by European initiatives such as the BEinGRID project (www.beingrid.eu).

Finally, business demonstration scenarios have been defined, in consultation with the product groups and lines of business of project partners. Achieving validation by means of successfully implementing and exploiting the identified business demonstration scenarios is the ultimate objective that remains to be achieved by the TrustCoM integrated project.

Bibliography

1. **TrustCoM deliverable D2**:"State-of-the-art evaluation", Emil Lupu (editor)
2. **TrustCoM deliverable D3**:"Case study scenarios", Paul Kearney (editor)
3. **TrustCoM deliverable D6:** "Roadmap of technical standards development v1.0", Joris Claessens (ed.)
4. **TrustCoM deliverable D7**:"Market Study", Yücel Karabulut, Jakka Sairamesh (editor)
5. **TrustCoM deliverable D9:**"TrustCoM reference architecture, version 1", Lutz Schulbert (editor)
6. **TrustCoM deliverable D10**:"Baseline Prototype infrastructure for CE scenario", Dave Golby (editor)
7. **TrustCoM deliverable D11**:"Baseline prototype infrastructure for ADP scenario", Tomas Garcia (editor)
8. **TrustCoM deliverable D14**:"Report on socio-economic models", Jakka Sairamesh, Jonathan Sage (eds)
9. **TrustCoM deliverable D15**:"Report on legal issues", Tobias Machler (editor)
10. **TrustCoM deliverable D16**:"TrustCoM Conceptual Framework - version 1" (July 2005)
11. **TrustCoM deliverable D18**:"TrustCoM Framework Specifications - version 1" (July 2005)
12. **TrustCoM deliverable D19:**"Basic set of TrustCoM methods & support tools" (July 2005).
13. **TrustCoM deliverable D22:** "Scientific and Technological Roadmap and Assessment of the project", Theo Dimitrakos (ed.), July 2005
14. **TrustCoM deliverable D25:**"Exploitation plans of identified innovations" Yücel Karabulut, (ed.)
15. **TrustCoM deliverable D24**:"Roadmap of technical standards development, v2.0", Joris Claessens (ed.)
16. **TrustCoM deliverable D37:** "Migration and Demonstration Plan for EC Demo, D. Golby (ed.), July 2006
17. **TrustCoM deliverable D38:** "Migration and Demonstration Plan for AH Demo, P. Kearney (ed.), July 2006
18. **TrustCoM deliverable D42:** "Enhanced Prototype of AS Scenario", Ignacio Soler (ed.), July 2006
19. **TrustCoM deliverable D43:** "Standardisation Roadmap, v3", Joris Claessens (ed.), May 2006
20. **TrustCoM deliverable D53:** "Methods and Tools", Alexey Orlov (ed.), July 2006
21. **TrustCoM deliverable D59**: "Socio-Economic Issues", Jaka Sairamesh (ed.), July 2006
22. **TrustCoM deliverable D60:** "Legal Issues", Tobias Mahler, July 2006
23. **TrustCoM deliverable D62:** "Framework V3", Michael Wilson, Lutz Schubert (ed), July 2006