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 .

© Copyright 2005 Atos Origin on behalf of the TrustCoM Consortium (membership defined above).

Neither the TrustCoM Consortium, any member organisation nor any person acting on behalf of those organisations is responsible for the use that might be made of the following information.

The views expressed in this publication are the sole responsibility of the authors and do not necessarily reflect the views of the European Commission or the member organisations of the TrustCoM Consortium.

All information provided in this document is provided 'as-is' with all faults without warranty of any kind, either expressed or implied. This publication is for general guidance only. All reasonable care and skill has been used in the compilation of this document. Although the authors have attempted to provide accurate information in this document, the TrustCoM Consortium assumes no responsibility for the accuracy of the information.

Information is subject to change without notice.

Mention of products or services from vendors is for information purposes only and constitutes neither an endorsement nor a recommendation.

Reproduction is authorised provided the source is acknowledged.

IBM, the IBM logo, ibm.com, Lotus and Lotus Notes are trademarks of International Business Machines Corporation in the United States, other countries or both.

Microsoft is a trademark of Microsoft Corporation in the United States, other countries or both.

SAP is a trademark of SAP AG in the United States, other countries or both.

'BT' and 'BTexact' are registered trademarks of British Telecommunications Plc. in the United Kingdom, other countries or both.

Other company, product and service names may be trademarks, or service marks of others. All third-party trademarks are hereby acknowledged.

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:	**7.1**
Work Package:	**12**
Task:	**12.1-4**

Document title:	**Progress Assessment and S&T Roadmap**
Version:	**1**
Document reference:	
Official delivery date:	**31 July 2005**
Actual publication date:	
File name:	**TrustCoM.D22.SnT.Roadmap.V2**
Type of document:	Report
Nature:	Restricted

Authors:	Theo Dimitrakos (BT) based on input from Alvaro Arenas (CCLRC), Philip Robinson (SAP), Johen Haller (SAP), Lutz Schubert (HLRS), Pablo Giambiagi (SICS), Christian Geuer-Pollmann (EMIC), David Chadwick (U. Kent), Emil Lupu (ICSTM), Babak Sadighi (SICS), Tomas Garcia (ATOS), David Golby (BAE Systems), Joris Claessens (EMIC), Jakka Sairamesh (IBM), Tobias Mahler (NRCCL), Fredik Vraalsen (SINTEF).
Reviewers:	David Golby (BAE Systems), , Emil Lupu (ICSTM), Stefan Wesner (HLRS)
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

Table of Content

1 About this document 7
1.1 Outline of this deliverable 8
2 Introduction 9
2.1 Towards the TrustCoM scientific & technological roadmap 9
3 Main Research Challenges and Project Scope 13
3.1 Main outputs of the TrustCoM project 13
3.2 Examples of Virtual Organisations 14
3.2.1 Virtual Organisations in Collaborative Engineering 14
3.2.2 Virtual Organisations for Next Generation Service Providers 14
3.3 Main research Challenges and Anticipated Innovation 15
3.3.1 Specific areas of innovation 16
4 Refinement and decomposition of the main technical research challenges 18
4.1 RC1: General Objective 18
4.2 RC1: Common ICT infrastructure for Virtual Organisations 18
4.2.1 Emerging solutions and trends 19
4.2.2 Open standards and common design patterns 20
4.3 RC2: VO management capabilities 20
- The means of modelling and representing the structure of VO have to be investigated 20
4.3.1 Emerging solutions and trends 21
4.3.2 Open standards and common design patterns 21
4.4 RC3: SLA and Contract Management 21
4.4.1 Emerging solutions and trends 22
4.4.2 Open standards and common design patterns 23
4.5 RC4: Trust & Adaptive Security 23
4.5.1 Emerging solutions relating to adaptive security and federation 24
4.5.2 Emerging solutions and trends on trust management 25
4.5.3 Open standards and common design patterns 25
4.6 RC5: Collaborative Business Processes 26
4.6.1 Emerging solutions and trends 27
4.6.2 Open standards and common design patterns 27
5 TrustCoM Framework: an overview 29
5.1 Enterprise Network versus Virtual Organisation 29
5.2 TrustCoM Framework subsystems 29
5.2.1 Virtual Organisation Management 29
5.2.2 Business Process Enactment and Orchestration 29
5.2.3 SLA Management 30
5.2.4 Trust & Security Services 30
5.2.5 Policy 30
5.2.6 VO Infrastructure 30
6 Projected timescales 31
7 Progress assessment 33
7.1 VO Management 33
7.2 Business Processing 33
7.3 SLA Management 34

7.4 Trust & Security Services 34
7.4.1 Trust & Security: Security Token Services 34
7.4.2 Trust & Security: Reputation Service 34
7.4.3 Trust & Security: Secure Audit Web Service 35
7.4.4 Trust & Security: Trust Negotiation Engine 35

7.5 Policy 36

7.6 VO Infrastructure 37
7.6.1 Enforcement & Service Management 37
7.6.1.1 Capability deployment 37
7.6.1.2 Service Management 38
7.6.1.3 Adaptive Enforcement 39
7.6.2 Messaging 39
7.6.2.1 Notification 39
7.6.2.2 Messaging Service 39
7.6.3 Registries and Meta-Data Repositories 40
7.6.4 Common VO infrastructure transactions 40
7.6.4.1 Coordination Infrastructure 40
7.6.4.2 Service Instance life-cycle management 40

7.7 Integration 41

7.8 Open Standards 43

7.9 Application domains 44
7.9.1 Collaborative Engineering 44
7.9.2 E-Learning Services (ADP scenario) 45

7.10 Contextual objectives 47
7.10.1 Legal aspects 47
7.10.2 Socio-economic aspects 47

8 Recommendations 49

8.1 VO Management 49

8.2 Collaborative Business Processes 49

8.3 SLA Management 50

8.4 Trust & Security 50
8.4.1 Security Token Services 50
8.4.2 Reputation service 51
8.4.3 Secure Audit service 52
8.4.4 Trust negotiation engine 52

8.5 Policy 53

8.6 VO infrastructure 53

8.7 Integration 54

8.8 Open Standards 55

8.9 Application Scenarios 55
8.9.1 Collaborative Engineering 55
8.9.2 eLearning Services 58

8.10 Socio-economic aspects 58

8.11 Legal aspects 59

9 Conclusion 60

Bibliography 61

1 About this document

This document is the main deliverable of the TrustCoM WP12: scientific & technological roadmap. Work started at the beginning of the project (month 1) and will last until month 18, covering the whole duration of this implementation plan. 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 this objective falls within the same group of activities (AL7), it is addressed by a different deliverable, namely **D1: Problem definition**.
- It does not attempt to sketch the state of the art outside of TrustCoM and define how TrustCoM is positioned against the state of the art. Although this objective falls within the same group of activities (AL7), it is addressed by a different deliverable, namely **D2: State-of-the-art evaluation,** which periodically revisited during the life-time of the project.
- It does not attempt to analyse the relevant Open standards in the areas where TrustCoM is achieving technological advancements, nor does it offer a roadmap towards integrating or extending these standards. This is addressed by deliverable **D24: Roadmap of Technical Standards development**.
- It 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 deliverables **D7: Market Study** and **D25: Outline exploitation plans**.

At the first phase of the project (month 1 to month 18) 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 first phase 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.

Section 4 analyses, decomposes and refines the research challenges summarised the previous section and shows how these are addressed by each specific technical activity of the TrustCoM project.

Section 5 summarises a comparison of the updated research objectives and interim results of the TrustCoM project to the current state of the art in commercial products and applied research

Section 6 offers a graphical representation of the projected timescales of the TrustCoM innovation from conception to market penetration.

Section 7 summarises a self-assessment of the project and places emphasis on the advancement achieved so far compared to the current trends in each relevant area.

Section 8 provides recommendations to each technical activity, in order to ensure convergence and leverage on all relevant interim results in preparation for the second phase of the project.

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 chapter **Error! Reference source not found.** of this deliverable. 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 conducted in the second phase of the project.

2.1 Towards the TrustCoM scientific & technological roadmap

This document is the main deliverable of the TrustCoM WP12: 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. D22 covers an assessment of M1-M18 and offers recommendations for the remaining of the project.

During the first phase of the project (month 1 to month 18), a particular emphasis is placed on achieving the necessary integration that would subsequently result in scientific advancements and technological innovation. 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 by WP11 during the first quarter of the project and results of the analysis have been documented in deliverable ***D3****: Case study scenarios*. The scenarios pursued in the remaining of the project amalgamate elements that have been identified as critical by this analysis.
    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 within WP10 and the results have been documented in ***D2****: State-of-the-art-Evaluation*. 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 preliminary standardisation roadmap was produced in the first year of the project (D6) and has been refined in ***D24****: Roadmap of technical standards development*. Standards cover areas from service management to identity management and federation, and from messaging to business processing. Similarly to D2, 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: AL1 that focuses on conceptual models and architecture and AL2 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 results of deliverables D2, D3 and D6 have been extensively discussed and accepted among all Consortium partners and in particular software vendors and end-users.

   b. Organised a series of detailed tutorials and panel discussions during the 2nd international conference on Trust Management (iTrust 2004),[1] in April 2004 where the targeted application domains, evaluated technologies and relevant standards were discussed with the community.

   c. Organised a panel discussion for feedback on initial results during a workshop at the 18th IFIP World Computing Congress in August 2004.[2]

   d. Organised two workshops with extensive presentations of research challenges, plans and results of the evaluation during the eChallenges conference in October 2004 [3]

   e. Participated at the DG INFSO Enterprise Interoperability Cluster and the Grid Concertation events.

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 during the first year of the project 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 during that period on experimenting with enabling technologies on diverse platforms (Java and .NET based Web Services) in order to assess the feasibility of prototyping these aspects. The results of this exercise lead into three main results:

---

[1] The first three International Conferences on Trust Management have been supported by the iTrust working group, which was a FP5 Thematic Network funded under the FET programme of IST. The iTrust network continues its operation after the end of the FP5 project and currently brings together over *100 researchers* from over *60 institutes* in Europe, America, Australia and the Far East. For more information on the FP5 project see http://www.itrust.uoc.gr. For information on the TrustCoM events see http://www.trustmanagement.clrc.ac.uk/ and http://www-rocq.inria.fr/arles/events/iTrust2005/ for the 2004 and 2005 events respectively.

[2] See http://www.wcc2004.org and http://www.wcc2004.org/congress/workshops/ws4.htm

[3] See http://www.echallenges.org/2004/ for the eChallenges event. The Workshops were 3e and 4e: “Towards a Trust & Contract Management Framework for Dynamic Virtual Organisations” 1 & 2. See also http://www.echallenges.org/2004/PDF/Workshop_3E.pdf and http://www.echallenges.org/2004/PDF/Workshop_3E.pdf

a. The identification of six subsystems for the TrustCoM framework blueprint. These are summarised in Figure 1 and described in more detailed in section 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.

c. The recommendation to the TrustCoM project management to radically change the project implementation plan of the main action lines under which research and technological development work is conducted (i.e. AL1 and AL2) in order to achieve a better alignment with the above structure. Following this recommendation the Consortium performed a *major project restructuring* at the end of the first year of the project.

   This restructuring effectively transformed the project from a generic "horizontal" structure that was looking into the "conceptual models", "architecture", "interoperability profiles" and "tools & methods" of the overall TrustCoM Framework, as depicted in Figure 1, into the more specific "aspect-driven" structure depicted in Figure 2 where technical workpackages directly correspond to the subsystems that have been identified. Each of these workpackages focuses on analysing, designing and implementing the key functionalities expected by each subsystem. For convenience, the division between modelling and prototyping activities has been maintained at a high-level although all the modelling and prototyping activities are now closely aligned for each aspect of the TrustCoM framework.

4. At a second phase, we expect to validate our interim results and revised objectives, resulting from the above. This second phase of validation involves

   a. A detailed tutorial at the 3rd international conference on Trust Management (iTrust 2005), in April 2005 where an update of the research challenges in view of the interim project results was discussed.

   b. A detail 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.

   c. Validation and further input from externals in

      i. DG INFSO Enterprise Interoperability

      ii. The Global Grid Forum

      iii. The project's technical advisory board

      iv. Other selected related initiatives in Europe and worldwide

The purpose of this second phase evaluation is to complete and update the research challenges based on the recent project evolution and experiences. An assessment of the project achievements will be provided in the final update of this deliverable towards the end of the project.

"Model driven security" is a separate area, yet closely linked to the other areas. Instead of addressing the functional and implementation aspects of the TrustCoM framework, this area addresses the design and development aspects that will be needed in order to easily build secure solutions using the TrustCoM framework. The project does not intend to start a standardization effort in this area. However, the security modelling languages developed are expected to provide a useful starting point for a potential future standardization effort. Experiences gained in model driven architecture may be used to validate and give feedback to emerging specifications.

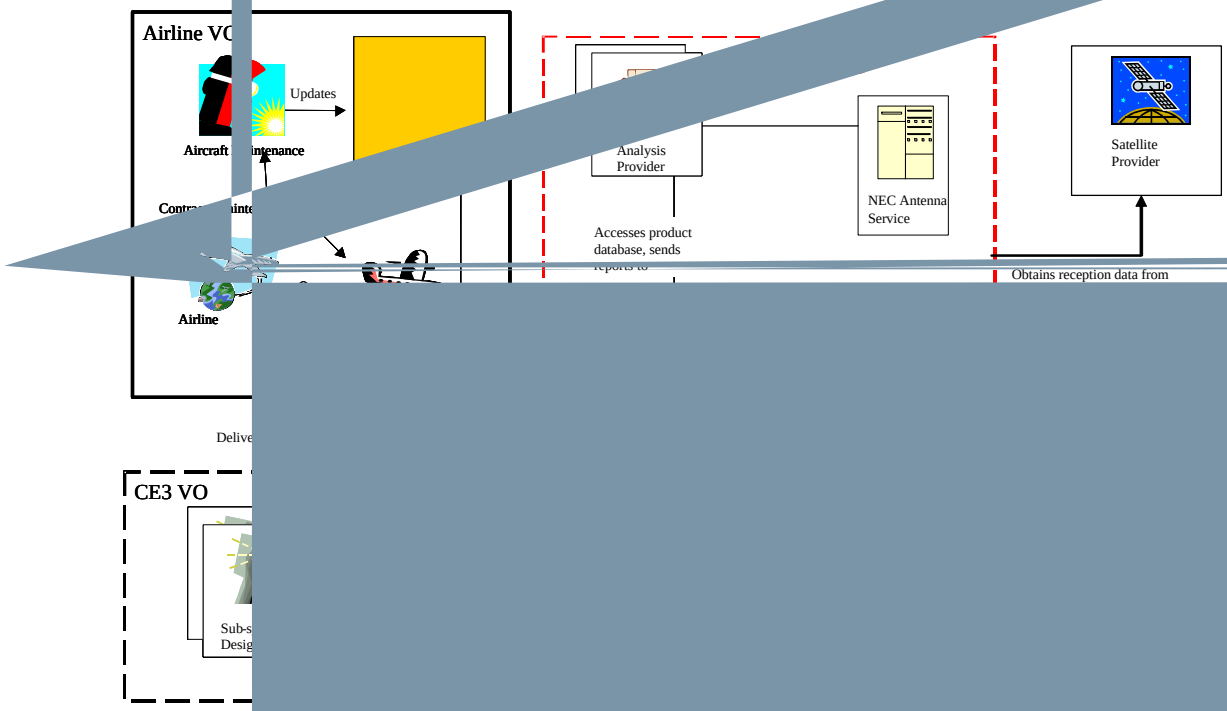
During the first phase of the project TrustCoM has disseminated its objectives and some early results into various, relevant standards initiatives (including IETF, ISO, GGF, OASIS, OMG), and has maintained a liaison with other projects in its area through the Cluster Enterprise Interoperability around the ATHENA project, and the Grid Trust and Security concertation.

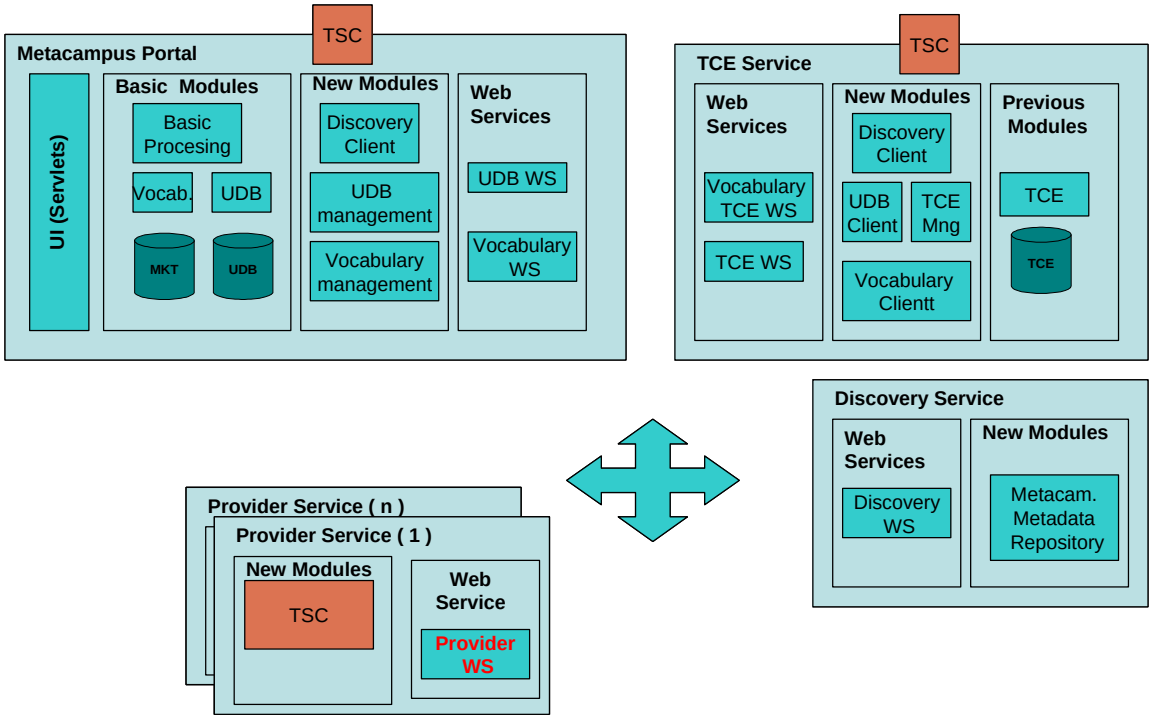
7.9 Application domains

Following an analysis of numerous scenarios in the selected application domains, the Consortium selected two scenarios, described in deliverables **D10** and **D21**, respectively. Although a critical mass of TrustCoM Framework services has not been integrated with these application scenarios as yet, the scenarios themselves exhibit distinct elements of innovation, relating either to the application of VO concepts in the respective domains or the re-engineering of their underlying ICT infrastructures so as to adhere to the basic principles of Service Oriented Architectures. In his section we summarise the main advancements to the state of the art that has been already achieved at the early stages of these testbed prototypes.

7.9.1 Collaborative Engineering

The main achievements in the first phase have been the development of an application scenario, the analysis of the scenario into collaborative processes, and the identification of the basic set of application services. A number of these application services have been implemented and are ready for testing in association with TrustCoM services. The services are currently deployed across three partner sites (Figure 7), as it is explained in TrustCoM deliverable **D10**: "Baseline Prototype Infrastructure for the CE Scenario".


Airline VO
Updates
Aircraft
Airline
Analysis
Provider
Accesses product
database, sends
NEC Antenna
Service
Satellite
Provider
Obtains reception data from
CE3 VO



The baseline prototype does not incorporate the TSC module yet. This module will implement the TrustCoM framework and supporting services. Following this new distribution from the Metacampus original platform we now have 3 distributed services:

- The *Metacampus marketplace*, which keeps the User Database and the Vocabulary Database that stores the Metacampus specific metadata related to competences.
- A *Training Consultant service*, that evolves from a simple module within the marketplace to become an independent service. This step will provide strong benefit to the marketplace as many vendors could implement different Training Consultant services working with the marketplace in competition by offering aggregated services.
- A *discovery service* that will substitute the Learning Resource Catalogue, which will store the metadata description of the learning resources published by the service providers with reference to the access web service (stored in a UDDI).

For the baseline prototype, which does not interface any TrustCoM specific subsystem yet, the major enhancement that it has been re-engineered in order to follow Service-Oriented Architecture (SOA) principles and take advantage of a network-centric Application Service Provision business model. The separation of concerns between the main business functions, their encapsulation into services and their exposure by means of programmable Web service interfaces reflects how we expect future network-centric systems to be built and provides a fertile ground for making most out of the use of selected services from the reference implementation of the TrustCoM Framework.

In parallel and implicitly there are other novel service interfaces that need to be created in order to communicate these new distributed services.

All Learning Resource Providers (LRP) will also have to implement a web service to provide the requested learning resource when invoked.

7.10 Contextual objectives

7.10.1 Legal aspects

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 and WP 9's focus is on the legal risks that may arise for participants in VOs. The work has been performed in close collaboration with other TrustCoM partners, in particular in relation to the TrustCoM scenarios on collaborative engineering and e-learning. This work has contributed to the overall TrustCoM framework by defining some legal requirements for trust, security and contract management in VOs.

This activity applies legal risk management as a novel methodology to analyse legal issues related to trust, security and contracts in VOs. The utilization of methods from legal risk analysis has allowed the team 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 has facilitated the integration of the perspectives of trust and security with the focus on legal issues related to virtual organisations.

The legal research performed 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 AS / eLearning scenario focused on legal risks related to international issues, i.e. choice of law and jurisdiction.

The workpackage is also developing methodology and tools for legal risk analysis. In particular, a graphical language is being developed which extends the Unified Modelling Language (UML) with relevant legal concepts, in order to make it more suitable for documentation and communication of legal risks and treatments. The utilisation of UML also ensures compatibility of the legal study with the work of the other TrustCoM partners. Work on formalising the language semantics is undertaken to make it more precise and to facilitate the development of automated tools for processing the graphical models.

7.10.2 Socio-economic aspects

Midway in the first year of the project, competitive game models were applied for VO selection and trust enablement between two parties. The models developed were focussed on individual trust models when compared to the requirements of the complex VO lifecycle management, which involves complex relationships between the VO members (group level trust). The game model was applied on a few attributes of the members and deeper insights into VO management were not revealed. One of the primary reasons was that the VO management framework was in the design stage and not fully conceived. Furthermore, focusing overall the priorities of the Consortium towards areas where a significant impact could be achieved in shorter timescales, meant that the Consortium were more interested on investigating the Business Models that underpin VO configurations where different trust relationships can be identified as well as exploring business contracts, an important area that could not be fully addressed, in the more technical part of the TrustCoM Framework (cf section 4.4).

Following the TrustCoM review done in April, 2005 the socio-economic team re-assessed their plan with the help of the TrustCoM Scientific Coordination and Programme Management, and the Consortium agreed on a set of modified objectives for November 2005 towards models of Reputation, Business models for Trust and others. The final modified objectives are as follows:

1. Explore advanced multi-tier Models of Business Contracts for VO Management

2. Economics of Business Contracts and Terms and Conditions for Reputation
3. Investigate models for Reputation based on metrics defined around contract terms and conditions. Investigate advanced scoring models for Reputation.
4. Investigate Business Models for Trust and Interoperability between VO members and other VO organizations.
5. Investigate Business models for Trust in third-party neutral or dominant group environments.

The socio-economic research team worked closely with AL1 and AL2 sub-projects and teams on Business Contracts, Terms and Conditions, VO management and Business Metrics for Reputation and VO supply-chain models. Work on Business Contracts has contributed knowledge and criteria to the TrustCoM framework subsystems. Currently a working group has been established to investigate role of Business Contracts in VO supply chains and in designing reputation mechanisms. The IBM team also intends to provide advanced knowledge, definitions and mechanisms around Business contracts, which will encompass the SLA work that is being done elsewhere in the project.

The team also provided input on “Generic Reputation Service” which is an important part of the VO lifecycle management and Trust/Security Services. The input has been on supply-chain metrics and contract attributes and management for building an industry driven reputation system. The socio-economic research team has also provided input to VO management (on Reputation scoring) on reputation models and scoring functions for VO members in a VO environment.

During the first phase of the project, the team working on socio-economic aspects developed a model of Business contracts for enabling VO supply chain interactions based on terms and conditions between VO supply chain partners. This is detailed in section 3 of D14: Report on socio-economic models

The team also developed novel reputation model based on Business Contracts and contract-specific terms and conditions. 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. The contracts signify the agreed upon terms, which if violated the conditions apply. Business rules can be set by the VO members on the violations to understand and select out the VO members. This has been accompanied by new 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. For example, in a VO supply chain if a VO member violated a specific term and condition 5 times then the scoring function will rate the VO member based on the type of term and condition. 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.

Economics and business models for Interoperability were developed as a part of the project’s socio-economic research activities. The models for interoperability consider trusted third-party, trusted consortia and trusted group models. The business models were compared and contrasted around various degrees of trust and reputation (this study was presented at a cluster interoperability workshop).

Other contribution includes offering advice on standards for business contracts, models for the Enterprise Interoperability Cluster of FP6 projects.

8 Recommendations

In this section we conclude the self-assessment presented in this deliverable by summarising specific actions that have been recommended to the TrustCoM consortium for the second phase of the project in order to for the project to tackle the research challenges outlined in section 3.3 and the specific scientific and technological development goals set in section 4. Where appropriate we highlight goals that fall outside the programme of the project and will have to be addressed by other research projects.

8.1 VO Management

In relation to VO Management, the TrustCoM consortium should aim at producing three components covering the essential requirements of a VO Management system: lifecycle management, membership management and GVOA management. Such components will enable the management of dynamic VO, taking into account trust and security constraints.

It has been identified that no VO Management product exists today covering these important issues (see Section 4.9 of deliverable **D25**, the exploitation plan). In order to realise this vision, we will implement a VO management subsystem covering the full cycle of a VO, concentrating in particular on the evolution phase of the VO lifecycle.

The relevance of semantic technologies for VO management has been identified. Semantic technologies have been found particularly useful for representing VO structure and dependencies between VO partners as well as offering a common foundation for processing. Current resources and priorities in TrustCoM do not allow an adequate investigation of the use of semantic technologies for VO management and GVOAs. It is recommended that further research relating to the use of semantic technologies for modelling VO management structures and GVOAs is conducted outside of, and where appropriate, in relation to TrustCoM.

8.2 Collaborative Business Processes

The collaborative business process models identified so far should be refined during design and implementation in two directions. First, the operational components, such as services, have to interface with other subsystems. These interfaces need to be defined, reviewed, implemented, evaluated and improved based upon experience and feed-back. Furthermore, a common and simple deployment process for all components including the additions to existing technology in the form of TSC extensions has to be developed. The TSC extensions also have to interface with other subsystems. Again, these interfaces need to be refined. Details of TSC extensions, such as their representation in public and private business processes need to be defined. A final implementation of the BP Enactment and Orchestration subsystem with the identified components and interfaces is supposed to be finished at conclusion of the second phase of the project.

Because of a change of priorities within the consortium and also because of the immaturity of technologies relating to technology for implementing choreographies of Web services, it has not been possible to properly address self-adaptive processing at all layers. It is recommended that further research relating to self-adaptive implementation of choreographies is commenced outside of, and where appropriate in relation to, TrustCoM. In the context of TrustCoM it is recommended that the focus shifts on the use of mechanisms for adaptation policies (such as those presented in section 7.5) and distributed transaction mechanisms (such as those presented in section 7.6.4.1) in order achieve some level of adaptation during the enactment of orchestrated business processes. Further research will also be required in order to correlate business process goals with security policies and SLA obligations. Also in this area the complexity and immaturity of enabling technologies in combination with limitations on resources has necessitated scaling down the ambition of the original project objectives, which however remain relevant research challenges.

8.3 SLA Management

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, negotiation of SLA terms, 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, but 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
- Implement a template repository that can be queried for discovery
- Develop negotiation services that are capable of agreeing upon SLA parameters using a fairly simple protocol. The discovered SLA templates will serve as a basis 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.
- Realize an SLA Manager service 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 a federation of services, operating on different administrative domains.

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 community supports further research in this direction. Such research will also have to take the legal implications of technology-driven automation into account.

8.4 Trust & Security

8.4.1 Security Token Services

Our main goal for this project is to implement an intuitive security management model that support humans in controlling *their* part of a virtual organization. In today’s IT systems, it is difficult to achieve a constant level of security. The limiting factor in maintaining consistent system security settings is the complexity of the security management. It is increasingly difficult for users and administrators to understand the implications of their daily security decisions. We already have designed a security management model and have implemented a first proof-of-concept prototype. The configuration of this first prototype is rather static, which shows that the cross-organizational service invocations work. However, it does not yet fully support the security management aspects. In the second phase of the project, we will provide management functionality for security token services and improve the implementation, as outlined below.

- We will use interoperable security token types. It is critical for the success of TrustCoM that we provide security token formats for cross-organizational service invocations, which are usable within a wide range of scenarios. In the first prototypical implementation, we used simple self-defined claims and attributes inside the security tokens. We will replace these claims by already existing claim and token formats, such as SAML/XACML, in order to re-use existing technologies as much as possible.
- The administrative interfaces in the first implementation of the security scenario are purely web service based and only support management through custom applications running on the client. In addition to these web service interfaces for autonomic security management, we will create web applications (HTML interfaces) that support business people with the administration of security-related aspects of their part of the VO.
- The first security scenario STS prototype (as implemented in mid-July 2005) solely performs authorization as part of the STS, i.e. we did not yet integrate the authorization process with the policy decision points (PDP) provided by the policy work package WP32. The next step before the review demonstration in October 2005 is to link these building blocks together. The implementation will support multiple deployment alternatives, i.e., we will support multiple interaction patterns between policy enforcements points, policy decisions points and STSs.
- The STS-internal configuration currently is based on plain text files, i.e. the management implementation currently does not provide sufficient and fine-grained access controls. The internal STS data structures should persist inside a scalable and manageable system, such as a database.

In this area TrustCoM anticipates offering fairly mature and generic technologies for supporting secure federation and the distribution. TrustCoM will not fully tackle however schemes for representing, processing and translating such credentials. Again 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.

8.4.2 Reputation service

Additional functionality that needs to be included in the system is the creation of an *electoral role*. This is important as it will allow the reputation system to record which actors are allowed to express the reputations of other actors. This will be achieved by linking the VO management and SLA systems into the reputation management system. We also want to *link the reputation system into the authorization system*, so that authorization decisions can be made based upon the changing reputation (or trustworthiness) of the principal. Current authorization systems (also known as trust management systems) only work in binary mode, in that a principal is either always trusted or always not trusted. Linking this to a reputation management system will allow much finer grained authorization to take place based upon dynamic control of trustworthiness.

Finally we want to define the *TrustCoM reputation metrics*, which will calculate a partner's reputation based on how well they have performed in the context of VO transactions. This will require the definition of the attributes, their possible weightings, the algorithms for combining the weightings, and interfaces for setting and retrieving reputations based upon them.

Although the TrustCoM consortium anticipates providing the archetype of a generic reputation system and implement protocols that enable the collection of evidence and other information (e.g. recommendations) that is consumed by the reputation system, the consortium will not conduct in-depth research on the role of reputation in Virtual Organisations and/or on optimal models for computing and representing reputation information. We anticipate making a proposal in this field with the understanding that the further research will have to be conducted in order to validate, revise and improve this proposal.

8.4.3 Secure Audit service

By the end of this project, we want to be able to provide the secure audit web service through all three interfaces: Java API interface, a TLS-protected TCP/IP interface and a web service front end interface. A high logging efficiency is an important factor for the successful application of SAWS in virtual organisations. We hope the minimal logging speed for SAWS can be 500 log records per second.

Currently, symmetric secret keys and private keys are used in SASW and they are protected by a Java KeyStore in the format of JCEKS. Obviously this is a software-based key management method, and it may pose a security weakness in reality. The security of the keys is the most important security issue in SAWS. We will look into the possibility of using a hardware-based key management method based on Trusted Platform Module, so as to increase the security level of the key management in SAWS.

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.

8.4.4 Trust negotiation engine

A wider diffusion of trust negotiation mechanisms requires solutions for several issues. The first step is to disclose, as far as possible, the requirements that both negotiation parties are equipped with the same negotiation engine. To this end, it is necessary to separate the disclosure policy-driven negotiation engine from the protocol that the two parties conduct the negotiation conversation through. At the same time it is necessary to express and publish the negotiation protocol in a suitable way, so that a client can automatically generate at least parts of the code needed to implement the negotiation 'stub'. Secondly, we must enhance the flexibility of the trust negotiation, by defining different negotiation strategies. The third issue is to improve the protection of the disclosed policies.

In order to solve these issues, we recommend the following steps:

- To address the first issue, we plan to expose the trust negotiation functionality using standardized protocols, or extensions of them. Candidate protocol standards are WS-Trust, WS-Policy and WS-PolicyAttachement.
- To improve the adaptability of the trust negotiation and the protection of the disclosed policies, we plan to extend the current prototype by introducing new negotiation strategies. In particular, these strategies are '*suspicious'*, '*strongly suspicious'* and '*trusting'* strategies:

  1. If the '*suspicious'* strategy is adopted, the credential proof is always requested during the policy evaluation phase for each of the involved credentials.
  2. The '*strongly suspicious'* strategy is a specific case of the *suspicious* strategy. Under the '*strongly suspicious'* strategy, parties require attribute disclosure as the corresponding policies are satisfied.
  3. The goal of the '*trusting'* strategy is to speed-up the negotiation process whenever possible. This can be done using credential *suggestions*, to be described (and stored) in an additional component of the negotiation policy. The main advantage of this strategy is that, if used for all involved policies, it reduces by half the number of rounds to complete a negotiation.

  Overall, the second phase of the project will focus on the implementation of an engineered version taking into account the above mentioned points.

  Further research to clarify the use of Trust Negotiation in virtual organisations is required. We anticipate making a proposal in this field with the understanding that the further research will have to be conducted in order to validate, revise and improve this proposal.

8.5 Policy

Whilst the first phase of the project has focussed on conceiving the policy framework, its architecture and principles of operation, substantial work remains to be done towards its implementation. Currently, simple obligation policies can be defined and enforced and simple policy groupings can be realised. However, substantial work remains to be done in terms of:

- Distribution, implementation of relationships and interactions across policy interpreters.
- Precise definition of the policy specification language and adaptation of the existing toolset to the new notation.
- Translation between the policy notation and the XACML format used by the policy decision point.
- Working out the details of how dynamic attributes, policy and attribute revocation and organizational dynamics are best modelled and handled in the context of delegation and policy administration.
- Enactment of the two project scenarios in this framework.

Thus, in summary, the second phase of the project will focus on the implementation of the policy sub-system as described in deliverables **D16**, **D9** and **D18**. This may require refinement of the models and architecture where appropriate.

8.6 VO infrastructure

In the first phase of the project a number of infrastructure capabilities have been identified. If these are implemented and integrated, the VO infrastructure developed in TrustCoM will offer substantial technological advancements compared to the majority of existing ESB and service management platforms. The main VO infrastructure capabilities that have are still in early phase of design and prototyping include:

- The messaging infrastructure, including support for advanced message routing and support for implementing different types of reliable message exchanges, based on explicitly defined and extensive messaging policies.
- Mechanisms for providing service registries and federated meta-data repositories that maintain the configuration of and allow seamless access to the management interfaces of potentially large groups of transient service instances.

Further to the above, the existing VO infrastructure capabilities will be refinement. Refinement during the second phase of the project will focus on tackling the following priorities related to the VO infrastructure:

1. Improving the design and implementation of the adaptive enforcement mechanism by:
    a. Analysing the dependencies between different categories of interceptors and reflecting these in the Configuration Policy in order to improve the reliability of the infrastructure.
    b. Integrating the existing mechanism with services that implement higher-level adaptation policies. Such integration is a high priority because, if implemented, it has the potential to realise a major technology breakthrough towards providing a technological foundation for self-adaptation during VO operation.
    c. Selectively including interceptors to assist SLA monitoring and process enactment wherever these are made available by the teams working on the corresponding subsystems.
2. Improving service management mechanisms by exposing advance interfaces for human administrators and by enabling the efficient, automated management of potentially large groups of service instances distributed across multiple hosts.

3. Extending the basic transactions that underpin life-cycle management so that they include configuration of various supporting services, such as registries, token services, monitoring and SLA evaluation services, policy decision points and adaptation policy services.
4. At present the transaction mechanisms can deal mainly with interactions between persistent services (although these can interact for e.g. managing the life-time of transient service instances). Implementing transaction mechanisms that can deal with transient service instances requires a technology breakthrough that is within the scope and the abilities of the TrustCoM consortium. Further research in this direction will be conducted in the second phase of the project.
5. Capability exposure and service instance life-cycle have been implemented at present mainly for application services rather than supporting services, which are assumed to be persistent. Improving these mechanisms so that they can also be used for infrastructure or other supporting services will enable the creation of distinct instances of infrastructure capabilities for different Virtual Organisations. This is a major challenge that is yet to be addressed and an essential technology if the operation of multiple Virtual Organisations over the same ICT infrastructure is to be achieved.

Finally the different capabilities of the VO infrastructure need to be brought together so as to form a coherent platform that offers advanced ESB and service management capabilities.

8.7 Integration

Integration is the outstanding challenge that has yet to be met by the TrustCoM consortium. The following actions are recommended 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;

Meeting these distinct integration milestones is a major outstanding research challenge for the TrustCoM consortium.

8.8 Open Standards

A broad set of selected standards and specifications have impacted the development of the components in the first version of the TrustCoM framework. Potential standards contributions have also been identified as part of these developments. The next steps for pursuing standards contributions include:

- continue dissemination to, and collaboration with, other projects in this area, in order to promote the TrustCoM technology, get feedback, and further align work;
- further integrate and mature the components into application testbeds as to get a more in-depth common understanding and a first validation of the results within the project;
- concentrate on integration profiles, bringing together the isolated subsystem developments; while we have refined the potential standardisation contributions *within* each specific TrustCoM research and development area, the most immediate result of the TrustCoM standardisation activity is expected to be in the integration of existing standards *across* the different areas.

It is important to emphasise that TrustCoM is an *integrated* project addressing trust, security, and contract management, for collaborative business processing, as a whole, focusing on the relationships and interactions between, and integration of, these issues, rather than investigating each of these issues separately and independently. The primary focus of the TrustCoM standardisation activity is expected to be 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.

8.9 Application Scenarios

8.9.1 Collaborative Engineering

The main outstanding issues are:

1. The development of additional application services to support more extensive collaboration services.
2. The use of the application services within the TrustCoM framework.

The additional application services will cover other aspects of the design-cycle such as customer negotiation, design, document review and a further decomposition of the Analysis phase into sub-tasks which could be distributed over different partner sites. This would make the testbed much more realistic and relevant to current aerospace procedures. Other services which offer information and data services will also be deployed. These include a satellite reception service and a product information service provided by a component supplier.

The concrete targets for Phase 2 are therefore:
1. implementation of additional application services outlined above, and

2. the initial deployment of TrustCoM services to implement a first version of a TrustCoM Virtual Organisation.

Regarding the latter of the two targets, the following sections indicate how the TrustCoM sub-systems will be used within the CE testbed.

- **EN/VO infrastructure.** We expect that for the CE scenario the EN/VO infrastructure will provide the following capabilities:
  - Service Instantiation: The NEC Antenna service is a good first candidate for demonstrating how a 'virtualisation' of services can lead to a more flexible VO operation that responds to varying customer demand. Issues to be addressed in relation to service instantiation include:
    - Establishing and managing the logical identity of the service instance
    - Offering values to agreed metrics for monitoring the service performance
    - Supporting the lifecycle of the application instance
    - Managing relationships to other service instances
  - The Policy Enforcement Point. The use of PEP will be important in enforcing security policies- a high priority in Industrial applications. The PEP of the service instance will intercept SOAP messages in order to:
    - Monitor invocations of the HPC Service
    - Enforce access control decisions- particularly important for the PDD, where different sections of the PDD will be subject to different access policies
    - Update the message header with new credentials and contextual information, eg, in accessing the PDD service or the product information service offered by a potential new supplier.
  - Notification: A certain number of services have an 'asynchronous' behaviour. A primary example of this includes the Analysis Service where invoking the service activates an internal business process that can be monitored using a 'handle'. This kind of behaviour is typical of many business processes where an incoming order is processed within some internal business process. In these situations, other services in a business process would wish to be notified when the associated task completes.
- **VO Management.** The CE Testbed will make use of the following components within VO Management:
  - Membership Management
  - Context Management (role & task management)
  - Choreography support

  In the current scenario, the assumption is that the CE VO is a pre-existing entity that accommodates new members and releases a number of these when the scenario goal is achieved. The management of this without the support of VO Management services would be expected to be highly labour intensive and time-consuming. Future editions of the Testbed will consider more interesting VO lifecycle use cases with more dynamic membership scenarios. For example, the members who are released at the end of the scenario include the Analysis consultancy and the NEC Antenna provider services who would be expected to receive payment for their services. Other transitory members do not expect payment, and these include the commodity component suppliers that join/leave the VO as the suitability of their offerings are assessed during the collaborative design process.
- **Business Processing.** Business Processing will be investigated in earnest in future versions of the CE testbed. In the present version of the CE testbed the business processes are only formally defined and managed 'out-of-band' of the collaboration. A more extensive design process will be implemented that will attempt to exercise this and the choreography aspects of the framework

- **Contracts and SLA**. The availability of reliable HPC resources are critical for the timely and accurate prediction of candidate designs. The introduction of the SLA will provide a step change over the current Grid model where issues such as SLA are resolved informally or by intervention of operatives. These the main services provided by the SLA Management module that will interface the application services:
  - **Monitors**: Relevant at different levels of the VO, depending on the functionality they provide: *Monitoring Interface* (so-called "Data Provider"), *Host Monitor*, *Domain Monitor***,** *VO wide Monitor* (so-called "Monitoring Aggregator"). In the CE scenario, and for the first iteration of its implementation the ***response time*** metric[20] will be critical for testing its functionality. Notably values for this particular metric can be provided either by explicit SLA monitors or by interceptors embedded within the enforcement mechanisms associated with the VO infrastructure.
  - **SLA Template Repository and Notary services**: both supporting services will store the SLA template associated with each kind of service provided. In the first case, the Service Provider, when publishing the service in the UDDI will also publish the associated SLA template with the relevant metrics and Quality of Service that the service offers. The Notary service will store the signed SLA agreed in the negotiation phase between the NEC Antenna service provider on behalf of the end user.

- **Trust & Security.** The general benefits are expected to be the management of resources within the CE VO that ensures data and service access to selected roles. This is a difficult and challenging topic for businesses that have extremely valuable IP but who wish to participate in different collaborations.

  The following table summarises the most important requirements that the application needs from the security & trust subsystem:

Entity	Requirement
End User & Service Providers	Single Sign-on Authentication Authorization and access control Reputation
Data (User Profile, LRP metadata)	Encryption
Orchestration (BPMS)	May require federated trust management May require data-level encryption and integrity control
Transactions	Digital signatures for non-repudiation (eg, in the case of uses of the NEC Antenna service)

  The issue of suppliers' Reputation will also be a topic for investigation. Reputation is important in establishing the most suitable supplier that could meet a sudden change in demand for a resource in the VO. A good example of this would for HPC resources, where one could have a large number of potential NEC Antenna service providers. Faced with a large number of suppliers who have the same technical capabilities, one would have to consider other factors that may be based on 'trust' or 'reputation' measures. Using Reputation one could have a much more open business environment in which new start up companies can quickly participate.

[20] ***Response Time:*** Response time is the time it takes the service to respond to a specific request. Normally, this is measured as the difference between the time the request was *sent* and the time the response was *received*. However, as this involves third party monitoring which is currently not present, we here simply return the temporal difference between the *ingoing* and the *outgoing* message – likewise, this value represents rather the processing time than the response time, but the metric itself can be easily reused for the first type.

- **Policy.** In addition to the specific targets related to authorisation and access control summarised in the pervious paragraph, the ability to make high-level policies that can be enforced throughout the infrastructure of the CE VO will be another important step change in capability.

8.9.2 eLearning Services

The Metacampus marketplace will be clearly enhanced with the TrustCoM framework services which will provide the current solution with the following new features:

- Adoption of a Service Oriented Architecture. Metacampus services will be deployed in different domains (service aggregator, Training consultant...)
- Learning Resources information distributed over different Service Providers
- Provide the application with trusted and secure services from Content Providers
- a new Discovery service to get up to date information of learning objects at the Service Provider sites
- Provide the Metacampus users with a more reliable and secure access control system
- A more dynamic and evolving service provision. Service providers will be federated as virtual organisations and the aggregation of services will clearly be more dynamic and efficient.
- A more flexible system for federation and registration of services
- A more powerful business process system to manage the provision of aggregated services
- A more user-oriented vision based on the negotiation and agreement of the service provision and quality of service
- Flexible and dynamic association between the different actors (SP, Training Consultants, users)

8.10 Socio-economic aspects

The following three major conclusions have been made through the socio-economic studies so far. Each of them requires a follow-up action.

1. *Economic models play a strong role in enabling trust mechanisms*. D?? describes the various economic and business models for enabling trust in third-party environments. The major result is that trust between parties or players is better when keeping a history of transactions. This was proven in several experiments that were conducted.

   Follow-up action: This result is being taken into consideration by the Trust & Security services subsystem where Audit and Reputation services have been introduced.

2. *Contracts are the life-line of building trust in Business Environments and VO supply chains systems*. Contract terms and conditions provide a tremendous foundation for Trust and Reputation management. The major result from the work is the design of a novel contract driven and attributes based reputation rating of partners in a VO supply chain. The reputation rating models consider attributes and criteria that are semantically driven.

   Follow-up action: the Reputation service considered under the Trust & Security workpackage should take these models into consideration and the SLA monitoring subsystem should offer the necessary information throughout the SLA life-cycle.

3. *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. These measurements will provide feedback into the generic reputation system models (section) for performing rating of members and new VO creation. The same applies to the subsystem addressing VO management and GVOA in particular.

   Follow-up action: the team working on the VO Management and SLA Management subsystems should consider the option of explicitly associating business metrics to certain terms and conditions described in the GVOA and SLA templates. The socio-economic team should refine the model and assist the other teams in defining concrete examples of such metrics.

8.11 Legal aspects

During the second phase of the project, the team working on legal aspects will continue to focus on the TrustCoM AS testbed scenarios, and in particular on access-rights management and also on the liability of VO participants in relation to access rights, e.g. how the access to resources in a virtual organisation may be legally classified and the effect this may have on the liability of its members. Legal risk analysis will be used both to identify legal risks and treatments relevant to VOs and to evaluate the suitability of the tools, method and language. Moreover, the work with methods for legal risk analysis for VOs will be finalized.

Regarding the TrustCoM CE scenario, the research performed in phase 1 identified the need for a more detailed legal analysis of confidentiality issues. This research will aim at identifying the risks to information that VO partners will have access to, with respect to (i) illicit access to confidential information by VO members or third parties, (ii) illicit dissemination of confidential information to entities that are not entitled to access the information. For a VO using the TrustCoM technology, the challenge will be to integrate the access based on policies as defined in the TrustCoM framework with the legal protection of confidential information. In this context the legal protection of confidential information in selected statutory laws will be analysed and the need for additional contractual clauses will be assessed. The analysis will include, for example, what is to be understood as confidential, how this information is to be identified in a web-services environment, how long the protection should last, procedures for lifting the limitation and procedures for exceptional circumstances.

9 Conclusion

As mentioned in section 2.1 of this deliverable, a interim progress assessment conducted by the project's scientific coordination and management teams during the first year of the TrustCoM project identified as a major risk the fact that the Consortium could be spending unreasonably large effort and resources getting deeper into a vicious circle of 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 new teams formed focused on delivery within their respective areas of expertise and, in particularly 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.

Notwithstanding this success, it is now felt that the TrustCoM consortium needs to find a way to build on this early success by successfully integrating their results instead of falling victims of their success by focusing on perfecting our current 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 subsystem by filling (at least) the identified gaps, the TrustCoM consortium needs to put in practice the so far top-down attempts to maintain cohesion across the TrustCoM subsystems, application scenarios and contextual research. In particular, the TrustCoM consortium needs to:

1. Understand the results of the legal and socio-economic research and selective use these results in those cases that they clearly add value.
2. Design and analyse integration scenarios for the TrustCoM framework subsystems. Then implement them bottom-up, starting by 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. Bring appropriate integrations of the TrustCoM Framework subsystems into the application scenarios and conduct a second of integration while ensuring the selection of services to be integrated is driven by the needs of each scenario
4. Document the findings of these integration attempts, and abstract application domain specific optimisation in order to produce "blue-prints" of the TrustCoM profiles.

Beyond and above 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.

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” (draft, July 2005)
11. **TrustCoM deliverable D18**:”TrustCoM Framework Specifications - version 1” (draft, July 2005)
12. **TrustCoM deliverable D19:**“Basic set of TrustCoM methods & support tools” (draft, July 2005).
13. **TrustCoM deliverable D25:**“Exploitation plans of identified innovations” Yücel Karabulut, (ed.)
14. **TrustCoM deliverable D24**:”Roadmap of technical standards development, v2.0”, Joris Claessens (ed.)