

Deliverable

D37

# Migration and Demonstration Plan for the Collaborative Engineering Demonstrator

**WP37** Collaborative Engineering Demonstrator

David Golby Editor

BAE SYSTEMS  
Advanced  
Technology Centre

2<sup>nd</sup> August 2006

V1.5

Contributors

Lutz Schubert (HLRS), Philip Robinson (SAP),  
Ignacio Soler (Atos Origin)

SIXTH FRAMEWORK  
PROGRAMME  
PRIORITY IST-2002-2.3.1.9



## **LEGAL NOTICE**

The following organisations are members of the TrustCoM Consortium:

Atos Origin Sociedad Anonima Espanola,  
Council of the Central Laboratory of the Research Councils,  
BAE Systems,  
British Telecommunications plc,  
Universitaet Stuttgart,  
SAP AktienGesellschaft Systeme Anwendungen Produkte in der Datenverarbeitung,  
Swedish Institute of Computer 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 Salford,  
International Business Machines Belgium SA .

© Copyright 2006 BAE SYSTEMS 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' is a registered trademark 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.

**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:** AL3 Demonstration Trials

**Activity:** Activity 3.1 Collaborative Engineering Demonstrator

**Work Package:** WP37 Collaborative Engineering Demonstrator

---

**Document title:** Migration and Demonstration Plan for the Collaborative Engineering Demonstrator

**Version:** v1.5

**Document reference:**

**Official delivery date:** 31<sup>st</sup> April 2006

**Actual publication date:** 2<sup>nd</sup> August 2006

**File name:** D37 Migration and Demonstration Plan.doc

**Type of document:** Report

**Nature:** Public

---

**Authors:** David Golby (Editor)

**Contributors:** Lutz Schubert (HLRS), Florian Kerschbaum (SAP), Philip Robinson (SAP)

**Reviewers:** P Kearney (BT), Pablo Giambiagi (SICS)

## **TABLE OF CONTENTS**

<b>Version History .....</b>	<b>8</b>
<b>Executive Summary.....</b>	<b>9</b>
<b>1 Introduction.....</b>	<b>11</b>
<b>1.1 Purpose of the CE Demonstrator.....</b>	<b>11</b>
<b>1.2 Objectives of the CE Demonstrator .....</b>	<b>12</b>
<b>1.3 Potential Contributions and Benefits of TrustCoM .....</b>	<b>12</b>
<b>1.4 Document Overview.....</b>	<b>13</b>
<b>2 Proposed Scenario and Key Questions .....</b>	<b>15</b>
<b>2.1 Proposed Business Scenario.....</b>	<b>15</b>
2.1.1 Business Model.....	15
2.1.2 Analysis of CE Test Bed Scenario .....	16
2.1.3 Summary of Changes.....	17
2.1.4 Scenario Description .....	18
<b>2.2 Stakeholders.....</b>	<b>20</b>
<b>2.3 Key Questions .....</b>	<b>23</b>
2.3.1 BAE SYSTEMS Key Questions.....	23
2.3.2 HLRS Key Questions .....	24
2.3.3 SAP Key Questions.....	24
<b>3 Migration Plan.....</b>	<b>25</b>
<b>3.1 CE Demonstrator Requirements .....</b>	<b>25</b>
<b>3.2 CE Demonstrator Model.....</b>	<b>26</b>
<b>3.3 Partner Responsibilities .....</b>	<b>27</b>
<b>3.4 TrustCoM Components and Prioritisation Issues .....</b>	<b>27</b>
<b>3.5 Plan.....</b>	<b>29</b>
<b>3.6 Experiments.....</b>	<b>30</b>
<b>3.7 Risks.....</b>	<b>31</b>
<b>3.8 Legal Issues.....</b>	<b>31</b>
<b>4 Demonstration and Reporting Plan .....</b>	<b>32</b>
<b>4.1 BAE Demonstration and Reporting Plan.....</b>	<b>32</b>
<b>4.2 HLRS Demonstration and Reporting Plan.....</b>	<b>32</b>

**4.3 SAP Demonstration and Reporting Plan .....33**

**4.4 Reporting Feedback.....33**

    4.4.1 Technology Level .....33

**4.5 Contribution to other initiatives .....35**

**5 Conclusions .....36**

**6 References .....37**

**7 Appendices .....39**

    7.1 Symbols Used in the Text.....39

    7.2 Appendix 1: CE Demonstrator Collaborative Business Processes .....40

## Glossary

An explanation of terms used within the document.

<b>Term</b>	<b>Description</b>
BPE	Business Process Enactment- the business process management sub-system in the TrustCoM framework.
CE	Collaborative Engineering
CFD	Computational Fluid Dynamics. The use of computers for the simulation of fluid (eg, air, water) behaviour. Used in weather forecasting, aerodynamics etc.
CEM	Computational Electromagnetic Modelling. The modelling of radar, antenna performance (mobile phones, aerials, radio etc) by means of numerical techniques similar to CFD.
CSM	Computational Structural Mechanics. The modelling of the effect of impacts (eg, bird strike), detonations etc on structures (buildings, planes etc) by means of computer based experiments.
EM	Electromagnetic, eg, EM Analysts- engineering specialists who analyse the performance of antenna or electronic equipment.
GVOA	General Virtual Organisation Agreement- an electronic agreement between partners containing the SLAs and policies that govern the VO.
HPC	High Performance Computing.
PDD	Product Design Database. A database for the storage, retrieval and tracking of all product-related information including customer requirements, designs, production-related specifications and product manuals.
SOA	Service Oriented Architecture. The software architecture based on the use of web-services for inter-enterprise business messaging.
STS	Security Token Service. Generates claims or statements about the originator of a web service message or of the provider of the service itself. Used for supporting federated Trust-based security within the VO.
TSC	Trust, Security and Contract. Used in various contexts eg, for denoting a service within the TrustCoM framework or a particular task or task role within the TrustCoM Business Management framework.
SLA	Service Level Agreement. The electronic agreement between the service provider and customer.

**D37 – Migration and Demonstration Plan****TRUSTCOM – 01945 02/08/2006**

CD	Collaboration Definition. A document that forms part of the VO agreement that binds the members together. It defines the information that specifies the business process choreography that the VO enacts.
ACL	Access Control List.
COI	Community of Interest. A particular interest group such as customers, system administrators, application developers, middleware providers etc etc.
TTP	Trusted Third Party.
SME	Small to Medium Enterprise.
VO	Virtual Organisation. A model of a collaboration that involves companies, academic institutions, governmental organisations sharing resources to achieve a common objective.
QoS	Quality of Service.

## **Version History**

Date	Description	Subversion Revision Id
01/06/06	Skeletal outline of the document, assigning partner's responsibilities etc	4391
14/06/06	Revised structure. Incorporates contributions from partners.	4388
16/06/06	Restructured again. Final structure to be approved by co-authors. Sections to be completed.	4525
20/07/06	Updated with components lists, prioritisation, model diagrams	5005
25/07/06	Updated with Executive summary. Released for internal review.	5059
02/08/06	Final version.	Latest edition



## **Executive Summary**

This document presents a plan to migrate the CE Test Bed developed in Action Line 2 to the CE Demonstrator intended for Action Line 3.

The objective of this study is to demonstrate an application scenario supported by TrustCoM tools. The demonstrator will attempt to give the best demonstration of TrustCoM technologies while also addressing the potential risks that are perceived by various stakeholders. This activity will also make recommendations for improvements in the post-project open source edition of the TrustCoM framework that is currently being planned.

The demonstrator will be based on a business scenario that is similar to that used during AL2. In this scenario, TrustCoM is seen as important in providing assurances in security, reliability (through agreed QoS) and manageability to these application services. The proposed application scenario will be based on provision of critical, inter-dependent application services to a customer in an engineering analysis consultancy. These services comprise the collaboration that will be addressed using TrustCoM tools.

The potential business benefit to the client in the scenario is the ability to reduce the administrative costs associated with the application by outsourcing capabilities to an external organisation that provides them as services. The requirements are that the service is easy to integrate into the client's own applications and business processes, has a well defined QoS, and has the required security policy. On the other hand, the business benefits to the service provider in the scenario includes the ability to aggregate computing resources and provide them to a wide community of users: management is maintained in-house and closely monitored. Requirements from his point of view are that the management costs are maintained at a low level when dealing with the many customers who require support for value-adding features such as QoS, security etc.

The current CE Test Bed scenario used in AL2 is analysed from the point of view of Business models and relationships, business performance, business reporting, outsourcing and application scope. Certain shortfalls that were identified include-lack of payment mechanisms, no transaction support, limited application service monitoring (only one at present...), lack of business reporting (critical for making correct business decisions) and lack of alternative service providers. The revised application scenario will attempt to address these shortcomings in order to remove any perception that the demonstrator is unrealistic.

We have tried to address end-user concerns by identifying key questions that potential stakeholders would be likely to pose. These stakeholders in the CE Test Bed are understood to be business decision makers, system admins, end-users, service providers and applications service developers.

From these key questions, a set of requirements were derived for the CE Demonstrator. These requirements include a) adopting a VO model of the

## **D37 – Migration and Demonstration Plan**

**TRUSTCOM – 01945 02/08/2006**

collaboration, b) a requirement to demonstrate how the VO is designed- ideally showing how the process of specifying it (eg, definition of GVOA) is currently supported within TrustCoM. During the operational phase, the demonstrator is required to show how events (such as changes in Reputation) are dealt with without disruption to the VO. It will also show how service providers that break the terms of their agreement with the VO can be replaced. An additional requirement is that the demonstrator should show realistic services, so we will attempt to use applications suitable for industrial design studies, such as the parallel version of the NEC code for example.

A basic model of the CE Demonstrator is presented showing the application service providers, client domains and trusted third parties. The TTPs are important ingredients of the scenario as they present possible business roles that may be present in future eCommerce environments.

We have identified all of the relevant TrustCoM Components and services that will be necessary for supporting the demonstrator. Given that time and resources may be limited, it is important to assign priorities based on current business objectives. The criticality of the TrustCoM components for the CE Test Bed has been classified as being of High, Medium or Low criticality. Critical components are those related to Security and require the highest priority during the demonstration phase. Medium critical components are those related to QoS and SLA support. Finally, the VO management has lowest criticality at present since the automation of service management is judged at this present time to have lower priority than security and quality of service. We view service management as important in the later phases of the deployment of SOA across a company when many services need to be supported across many different collaborations. In the near term, we assume that limited numbers of services will be used by companies as the security and reliability issues of SOA are understood and assessed. Once confidence in security and reliability has been attained then larger numbers of services will be deployed and service management becomes important. However, It should be noted that is our intention to demonstrate VO Management to best effect within the demonstrator as we see this as one of the distinctive contributions from the TrustCoM project.

A development plan has been proposed. During 2006 we will gradually expend effort on refining the requirements, conducting interviews with COIs and progressing any changes that are required in the application services. The results of the assessment exercise in AL2, and the recommendations from the Reviewers at the October Review will be input into a revised plan. We envisage that small, value-adding modifications to the presentational aspects of the TrustCoM tools - eg, management tools and so on will also be made.

Results will be reported to the TrustCoM project and disseminated to the EU Community and by each partner through other projects. The feedback provided by demonstrating the reference implementation will be used for deriving new requirements and identifying capability gaps of the TrustCoM framework.

# **1 Introduction**

## **1.1 Purpose of the CE Demonstrator**

There is an increasing need to automate, or at least make more efficient, business processes that span enterprises. These processes need to be adaptable and ready to change or be reconfigured as business partnerships change.

This in turn drives the requirement for greater integration of applications and information systems both between departments of a company and between different organisations. These systems may be new or legacy based and hosted on different platforms, eg, operating systems, servers etc.

Some examples of the scenarios where these integration challenges arise include:

1. the need to out-source IT services, such as storage, high performance computing etc as they are too expensive to maintain in-house;
2. the need to integrate enterprise applications such as human resource systems, project management systems, employee clock-in systems, customer relationship management systems etc in new ways to ensure information is up-to-date, consistent and available to a wide range of applications;
3. organisations involved in joint business ventures face the problem of how their resources can be effectively shared and co-ordinated in order to provide a more advanced capability than one that can be provided by an individual organisation. The choice may be in re-using existing in-house capabilities or building new systems for housing data and applications for the sake of protecting legacy systems, and
4. integrating suppliers' order systems with a customers stock purchase system as a first step in the automation of the purchasing process.

The concept of a Service Oriented Architecture (SOA) is seen as a flexible and more dynamic way of integrating the systems and applications together that are involved in these scenarios. Through this integration, automation of key business processes may become possible, thereby reducing costs.

There are, however, perceived risks to SOA, including security, reliability and manageability (amongst many concerns) that need to be addressed before the technology is adopted for mainstream use.

The CE Demonstrator will show how the potential benefits are feasible while showing that the perceived risks can be managed and contained. This will be done within a business prototype that shows how services of relevance to the design phase could benefit from TrustCoM.

## **1.2 Objectives of the CE Demonstrator**

The objectives of the CE Demonstrator are:

1. to demonstrate a plausible application scenario where external application services, provided by collaborators or software suppliers, are relied on to provide a critical capability to a design team
2. to demonstrate the benefits of TrustCoM when applied to this scenario in order to interest potential customers and other potential communities of interest
3. to promote the results of TrustCoM through various channels, including contributions to other initiatives and projects, where possible;
4. to provide steer to the future development of TrustCoM by posing new requirements derived from the business evaluation of TrustCoM, including feedback from its potential customers.

## **1.3 Potential Contributions and Benefits of TrustCoM**

In current eCommerce practice, business relationships and collaborations are built by traditional means, eg, face to face meetings, detailed contract negotiations are involved, systems are re-configured and proprietary infrastructures are used. In addition to this, the collaborations tend to be rigid and difficult to re-configure, eg, to replace suppliers or partners who are poorly performing- the 'passengers of the project'. As a result, collaborations are slow to build and complex to maintain.

TrustCoM is intended to support collaborations (modelled as 'Virtual Organisations') on the open Internet. The expectation is that it is intended to make the time for collaboration quicker, enable a wider (more competitive) pool of service providers offer their services and reduce the overheads for administering the collaboration.

TrustCoM provides an architecture for making the process of building and maintaining Virtual Organisations easier. The architecture re-uses existing standards to facilitate the implementation and leverage the use of commodity technologies. It also provides an open source implementation of parts of this architecture (the 'reference implementation'), that will facilitate the adoption of the architecture by many business application vendors. The toolkit is intended to provide an open source, basic capability that can be used for supporting online collaborations. The reference implementation will provide a means of identifying limitations of the framework through testing and experimentation and will provide the requirements to fill in 'capability gaps'. Optimised and value-adding implementations of the TrustCoM framework could be provided by commercial software vendors within their new or existing products.

The model of TrustCoM as from an end user perspective can be expressed as follows. A party who wishes to form a collaboration with well defined goals and objectives can use TrustCoM to locate a suitable choreography (designed by a

skilled operative within his own organisation or by a third party) which is stored in a repository. This document specifies the business roles within an overall collaborative process. The roles are essentially the services that provide a “product” or “capability” with a well defined interface, eg, an information service or as, in this particular case, a simulation capability. The implementation of these capabilities may be rather complex (eg, involves orchestration of complex internal processes) but these details are hidden from the client. These roles have input messages from other roles and provide output messages to other roles. Therefore, one has a chain of interdependent services, each provided by roles that participate in a collaborative business process. In the formation phase of the VO, each organisation agreeing to fulfil a role negotiates an agreed level of service and security policy. If this service level agreement is broken, then it has broken its contract and it may be liable for replacement. The VO agreement also incorporates policies, executed and administered by its internal systems, for dealing with exceptional events within the VO. Therefore, the whole collaboration is founded on a set of electronic documents (contained within the “GVOA”) that can be used to a) define the types of members involved, b) the agreements that bind them, c) the duties of each within the collaborative business process, d) policies for dealing with the evolution and management of the collaboration. The ultimate aim is to ensure that the electronic agreement can be used to configure and manage the service-based software systems that each partner uses, thereby reducing administration overheads.

<b>ID</b>	<b>Description</b>	<b>Key Benefits</b>
KB-1	Agreement driven, declarative model of VOs- the business roles, processes etc that promotes and facilitates the automation of repetitive business processes	Consistency between business objectives and computer system configurations, leading to improved communication between IT and business personnel.
KB-2	Agreement emphasis on the public duties of a business role, leaving private processes to be defined by the particular company that assumes the role.	Flexibility, controlled visibility of processes
KB-3	Membership based on capability and performance	Performance driven membership. Ensures that the collaboration can replace poorly performing partners without disruption to the VO

Table 1 Key Benefits from the TrustCoM Approach

## **1.4 Document Overview**

The structure of this document is as follows. The first section describes the business scenario to be used in the demonstrator and identifies the stakeholders and Communities of Interest in TrustCoM- the potential customers of TrustCoM. The key questions posed by these communities are posed along with the requirements on the CE Demonstrator to address these questions. The following section proposes a migration plan for addressing these requirements, describing how the current CE Test Bed will be taken over into an industrial prototype for Collaborative Engineering.

**D37 – Migration and Demonstration Plan**  
**TRUSTCOM – 01945 02/08/2006**

The plan for demonstrating and reporting the results of the work will be described in the final Section.

## **2 Proposed Scenario and Key Questions**

This section presents a basic business scenario for the demonstrator and identifies the stakeholders who would have some interest in this kind of scenario.

The previous section attempted to summarise what the key benefits of TrustCoM are intended to be. Given this ‘sales-pitch’, a number of potential stakeholders would pose questions of the benefits and risks involved with using the TrustCoM framework for their on-line business activities. The prototype must emphasise the benefits of SOA and show how the perceived threats can be effectively managed and contained in order for the promotion of TrustCoM to be successful.

This section attempts to identify these Key Questions based on the expected interests and concerns of the various current and potential Stakeholders in TrustCoM. It is expected that as the demonstrator progresses and feed-back from these end-users is obtained then these questions will be revised and refined and the contribution of the demonstrator becomes more apparent.

### **2.1 Proposed Business Scenario**

The purpose of this section is to present a proposed business scenario for the demonstrator. In accordance with the proposed ‘migratory approach’ of this activity (ie of reusing and extending work done in AL2), this will be based on the existing scenario in the CE Test Bed. This is reviewed and a set of improvements are proposed. The detailed description of the CE Test Bed scenario can be found in [1].

#### **2.1.1 Business Model**

The application scenario will focus on the dynamic, adaptive provision of a number of inter-dependent engineering services from various specialist companies. The basic assumption is that these services are expensive to maintain as in-house applications and therefore benefit from being outsourced to external providers. This approach reduces administrative costs to the customer and allows for better resource planning in the sense that sudden increased demand can be met by using other similar service providers. This model also ensures that service providers can exploit scalable, low cost computing platforms (eg, PC clusters) without any impact on a client’s own infrastructure.

The customers require various supporting services to integrate these services into their preferred in-house applications. These applications could range from conventional scientific/engineering products such as COVISE™ to more ubiquitous applications such as Microsoft Excel™. The range of customers varies from engineers who wish to use High Performance Computing (HPC) platforms for their design analyses to project managers and decision makers who wish to collect various resource data provided by the collaborators and suppliers. The expectation

is that the supporting services will enable Security and QoS requirements to be expressed and enforced.

From the service provider's point of view, the expectations are that the services are easy to administer and meet all possible aforementioned customer expectations.

The EN/VO infrastructure plays an important role in ensuring that these services are discoverable as a market of potential service providers. It facilitates the deployment of services, discovery of services and configuration of services for use in the wide range of application VOs that are possible.

## 2.1.2 Analysis of CE Test Bed Scenario

### **2.1.2.1 Business Model and Business Relationships**

A crude business model was adopted for the CE Test Bed that was expedient and fit for purpose in the context of the TrustCoM implementation phase. This involved an imaginary world of service providers- electromagnetic simulation, data storage- that collaborate to offer combined services that could be integrated into new engineering, business-hardened 'collaborative process' required by teams of designers in a collaborative project.

The demonstrator is intended to show the TrustCoM framework in a business context. Though the current CE Test Bed shows some aspects of this environment, further improvements are required to show:

1. more complex business processes, demonstrating how realistic, loosely coupled business interactions can be supported within the VO.
2. financial transactions that show a more realistic business relationship between the imaginary partners, and
3. the storage and retrieval of engineering process definitions that can be used for a collaboration by business designers.

In the aerospace sector, many issues that decide a business relationship are based on human judgement and are not considered to be within the management of software. Therefore, we do not expect that the VO management capability that TrustCoM offers would be appropriate for the management of processes and relationships at the very highest levels of the collaboration- eg, the overall design cycle- where human judgement is critical and where the scope for automation is currently limited. Instead, emphasis will be given to the management of lower-level services which are more suitable for use in a fully automated process.

### **2.1.2.2 Business Performance**

The scenario currently only includes one service whose performance is monitored. Business processes will typically depend on many services for their operation, so the system must demonstrate that more than one service can be monitored. It must



also show that the overall business performance is maintained and is supported by the automated management of service providers.

#### **2.1.2.3 Business Reporting**

Reporting the state of a project, or business process are very important inputs into the business reviews that are regularly held. Business reviews are important aspects of the overall business process and should be addressed. Therefore, the scenario is extended to include use cases where information generated within the VO, eg, within the SLA sub-systems, VO Management systems and Reputation systems etc, are retrieved and processed to give a view on the business status of the collaboration.

#### **2.1.2.4 Collaboration and Outsourcing**

Trusted Third Parties are important for demonstrating how essential capabilities for brokering trust, security, management etc can be provided by external companies. These show benefits to the consumer- simplified administration through outsourcing- and incentives for new or existing service providing companies. These represent service providers in their own right that have business motivations of their own that can foster collaborations.

Therefore, the above TTPs will continue to be used in the CE Demonstrator. This will emphasise the ability to outsource the VO administration and infrastructural services to external providers.

#### **2.1.2.5 Application Scope**

At the present time, the CE Test Bed has a limited number of possible application services for engineers to use. These are sufficient for development and testing of the TrustCoM toolkit, but a more convincing scenario should a) provide additional capabilities, and b) provide more than one service provider for a given type of service.

To make the pool of available services more diverse, additional application services developed for other EU-funded projects will be incorporated. These involve more services, enhanced automation, and industrial scale test models that will be more appealing to members of the engineering/aerospace community.

We will also use other partners to deploy alternative versions of certain services (such as the NEC antenna service) so that the VO evolution (eg, replacement of poorly performing service providers) can be enacted.

### **2.1.3 Summary of Changes**

<b>ID</b>	<b>Requirement</b>	<b>Proposed Change</b>
-----------	--------------------	------------------------

BR-1	Business Relationships	Payments should be part of the agreements, including penalties for violations.
BR-2	Business interactions	Discrete, robust, transactions should be demonstrated. Private/public views of the business process should be improved by incorporating additional services within internal business processes.
BR-3	Business reporting	The state of the VO should be observable and able to be reported to eg, finance and business decision makers in a tangible form to the relevant personnel.
BR-4	Business Performance	Additional SLAs need to be introduced, particularly for the Storage Provider (eg, response times)
BR-5	Management	The scenario will demonstrate a phased, adaptive response to changes and events and not an abrupt change that threatens the stability of the collaboration.  The scenario will demonstrate as much automation of the management of the VO as possible.
BR-6	Business Roles	The scenario will include TTPs, suppliers and consumers of services.
BR-7	Scope	The scope of the scenario will be improved by introducing more types of engineering services, eg in CFD, as developed in external projects.
BR-8	Market Aspects	Alternative service providers will be included using 'fake' versions of the application services

#### 2.1.4 Scenario Description

The Application Scenarios will be based on the existing CE Scenario but enhanced with additional 'business-focussed services' for billing, accounting and financial reporting etc. It will also introduce new application services introduced from other projects (such as SimDat) which will be of interest to other communities, such as in CFD.

As before, the scenario involves an existing VO that changes in response to a business opportunity. A prime partner, an aerospace company, has the concept of upgrading a particular product line in response to market requirements. A new member providing the required capability- in flight entertainment and internet access- is identified and enrolled into the organisation. The design of the platform now needs to incorporate this new sub-system and a design study is initiated to identify the costs and risks involved with the upgrade. At this point, the VO enrolls an additional set of members- engineering consultancies, scientific/application service providers, storage and data mining providers, etc- to analyse these designs. Their findings inform the business decision making and customer negotiations during which possible upgrade solutions are presented to the customer. When a design agreeable to all parties is achieved, the contract is awarded and the VO is

reconfigured to disconnect from providers of the services that were used for the analysis of the design proposals. Payment is made and contracts terminated.

The demonstration will simulate the full lifecycle of the VO that is formed from engineering services provided by a number of ‘synthetic companies’, ie, imaginary companies or entities as enacted by TrustCoM partners. These entities include academic research teams, in-house engineering applications and ‘commercial’ services provided by SMEs. It will show how the collaboration could be formally designed at a ‘top-level’ by the prime contractor (the ‘integrator’), and security policies, collaborative business process descriptions and SLAs are defined.

During the scenario, exceptional events surrounding the HPC service are envisaged and dealt with. This illustrates the ability of the VO to react to and manage services. First of all, falling Reputation of one of the engineering services (as reported by other users) prompts the engineering consultancy to enforce extra monitoring procedures. These are reported to the management in on-line reports. Another example involves an event where the SLA of the HPC service is broken - the quantity of agreed CPU reserved for the client is not met- and financial penalties are imposed. The service delivery is further compromised and the Service is then liable for replacement. The replacement process is initiated and the VO admits a new member.

The following diagram shows the various actors and roles within the scenario.

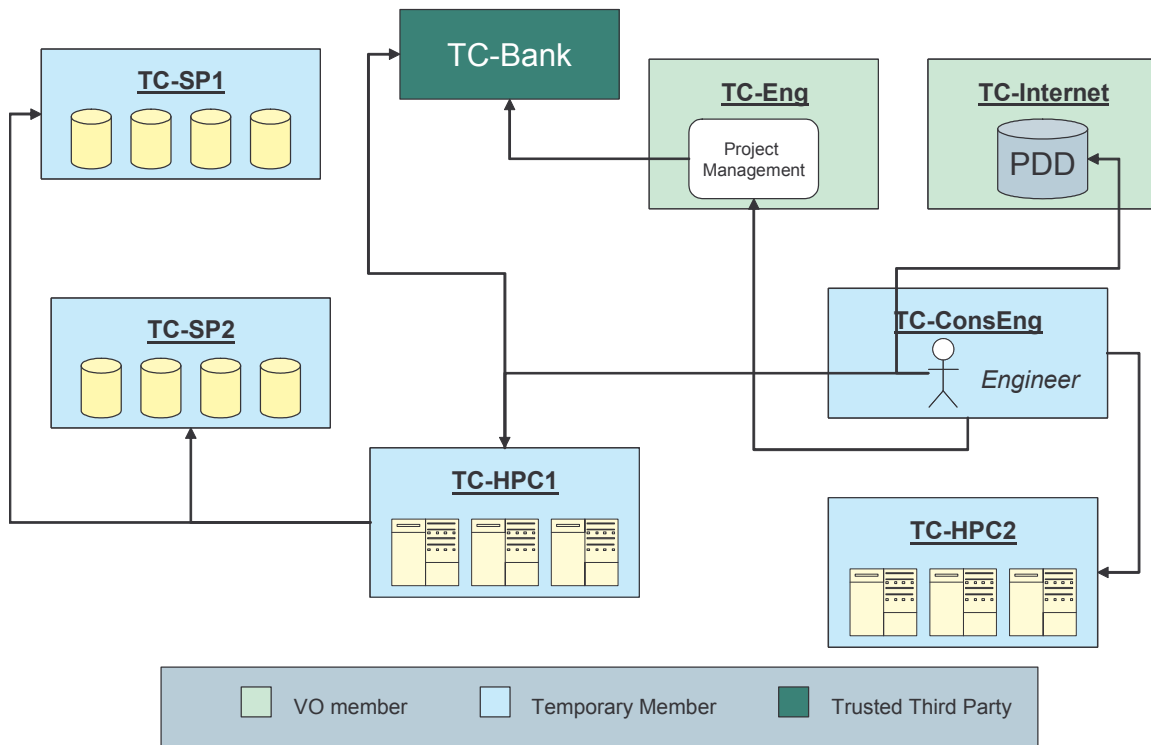


Figure 1 Demonstrator Scenario

The principal actor is TC-Eng, the ‘integration company’ which acts as the general project management function of the VO and which is aiming to win the contract. TC-Eng enlists the TC-Internet into the VO as a full-time member and as a major sub-system provider. TC-ConsEng is also enrolled as a temporary member and provides the engineering consultancy services, accessing design data from TC-Internet’s Product Design Database (PDD) system. Other organisations are also enrolled, including TC-HPC (a super computing and applications provider) and storage providers TC-SP1 and TC-SP2. Another application service provider, TC-HPC2, is selected for other engineering services, namely for fluid dynamics simulation. Finally, TC-Bank acts as the Bank to which use of the various services (such as TC-HPC1, TC-HPC2) by customers are charged.

Notable business interactions that are possible within the scenario include: a) Controlled access to the engineering data systems (such as the PDD), b) Billing and charging for use of services, and c) Reporting to project management systems d) notification of legal experts when agreements are broken.

Interaction a) involves the engineer accessing the PDD owned by TC-Internet. In this case, the engineer is allowed access and the data is returned in a response, but some sensitive information is removed from the message. Interaction b) is very critical and involves a transaction that needs to be reliable against failed connections etc. Interaction c) involves controlled access to another information system in a similar way to a). The final interaction involves the use of Notification to ensure that in the event of failures of critical points in the collaboration where human intervention is required then the correct operatives are alerted.

## **2.2 Stakeholders**

We now identify the potential stakeholders in the above scenario. Apart from the TrustCoM team (and associated researchers and technologists), there are various stakeholders who would be interested in the results of an industrial prototype based on TrustCoM. These are parties who are considering adopting SOA for facilitating enterprise application integration, the possibility of new revenue streams from exploiting internal capabilities, and improved integration with systems owned by partners and suppliers, etc.

These stakeholders include:

- **business decision makers** who are interested in integrating enterprise applications, extending the scope of collaborations with external companies, supply chain management etc and are considering the feasibility of using TrustCoM for supporting their work
- **system administrators** (both on the application and end-user sides)
- **end-users** - who put together a VO to service their needs- a new overall capability they require for a particular need;
- **service providers** departments in large organisations and SMEs who deploy services on the Internet for revenue

- **application service developers** who develop the services and who may have close associations with service providers.

Their concerns are related to the risks associated with security, service reliability (including the ability to deal with failures and poor service performance) and the management of an SOA to facilitate collaborations.

By partner, the identified stakeholders are shown in the following table:

**D37 – Migration and Demonstration Plan**  
**TRUSTCOM – 01945 02/08/2006**

<b>Partner</b>	<b>Stakeholders</b>	<b>Description</b>
BAE SYSTEMS	Advanced Technology Centre	End users, application service developers
	Airbus UK: Wing Design Team	End users, application service developers and service providers
	BAE Enterprise Integration Team	End users
	EXOSTAR: eCommerce	End users
	Corporate IT Services and Security	Decision makers and System administrators
	CFMS	End users, application service developers and service providers
	Suppliers of software tools to BAE	Application service developers
SAP	Internal Product Teams	Product and middleware developers
	NESSI	Product and middleware developers
HLRS	HLRS University of Stuttgart	Service providers and System Administrators
	Automotive companies, Engineering SMEs	End users
	Academic research groups	End users
Atos Origin	Internal Product and Services Teams	Product and middleware developers
	TrustCoM Open Source Management Team	Service providers
	NESSI	Product and middleware developers

In general, the expectations of these parties are:

1. **Developers**- ideally, no modification of application code or constraints on their service interfaces or implementations are required; any changes are required to be minimal
2. **Decision Makers**- the TrustCoM framework facilitates the collaboration making it quicker, has low administration costs, is secure
3. **Admins**- the TrustCoM services are easy to configure, offer flexible security
4. **End Users**- the VO is easy to design, define policies for, monitor, is autonomous and requires little intervention

## **2.3 Key Questions**

### **2.3.1 BAE SYSTEMS Key Questions**

<b>Key Question</b>	<b>Description</b>	<b>Stakeholders</b>
BAE-0	Can message security be enforced effectively within an organisational domain as well? How flexible is the PEP in this regard?	Decision makers, end-users
BAE-1	What are the potential business performance improvements from adopting the service infrastructures that TrustCoM is providing?	Decision makers
BAE-2	What are the potential cost savings from using TrustCoM to improve the outsourcing of engineering and business related services?	Decision makers
BAE-3	What changes to current IT infrastructures would be required to participate in the service-based economies that TrustCoM envisages? What are the 'entry costs' from doing this change? What skills would be required?	Decision makers, System admins.
BAE-4	How easy is it to set up collaborations using the toolkits and services that the reference implementation would provide? How powerful is the GVOA- can it configure everything in the VO? How much help is required?	End users, Developers?
BAE-5	How easy is it to deploy TrustCoM in accordance with business and organisational policies? What conflicts are likely to arise?	System admins
BAE-6	How flexible are the services and infrastructure to deploy and administer? What are their dependencies on other software and systems?	System admins
BAE-7	Are the tools robust and reliable? Are they difficult to configure?	System admins, end users
BAE-8	Can the framework be applied to non-trivial engineering applications? What is the scope of application to engineering problems involving the collaboration of many engineering services based on HPC platforms?	End users
BAE-9	How can service reliability be assured and what can be done in response to poorly performing services?	Decision Makers
BAE-10	Would existing security policies for IT infrastructures have to be modified to enable TrustCoM to be deployed in the business?	System admins
BAE-11	How stable is the VO to changes in membership, exceptional events and so on?	Decision Makers, end users
BAE-12	How are decisions requiring human judgement incorporated within the scenario?	System admins, Decision makers
BAE-13	How powerful are policy languages in the regulation of the VO?	System admins, Decision makers
BAE-14	How well is the management of the VO lifecycle automated and regulated on the user's behalf?	System admins

### 2.3.2 HLRS Key Questions

The key questions to be answered in this part of the demo include:

<b>Key Question</b>	<b>Description</b>	<b>Stakeholders</b>
HLRS-1	How effective and reliable are the underlying security services?	System admins
HLRS-2	How easy is it to integrate TrustCoM with existing resources?	System admins
HLRS-3	How easy is it to set up SLA contracts with customers?	Decision Makers, End users
HLRS-4	How reliable is the SLA management?	Decision Makers, End users
HLRS-5	How easy is it to maintain TrustCoM enabled HPC services?	System admins

Feedback from this exercise will also act as material for future research requirements in HPC provision and management. These include the areas of security, SLA and Reputation management.

### 2.3.3 SAP Key Questions

The key questions of interest where TrustCoM results can be highlighted include:

<b>Key Question</b>	<b>Description</b>	<b>Stakeholders</b>
SAP-1	What existing business models and needs can be supported by VOs and what new forms of business become economically viable using this technology?	Decision Makers
SAP-2	What are the inherent trade-offs in the technology and what range of different business models can be sufficiently addressed with one technical framework?	Decision Makers
SAP-3	What are the main cost drivers when using this technology and how can they be effectively addressed?	Decision Makers, End Users
SAP-4	How can the acceptance of this technology be increased in the market and organizational and socio-economic inhibitors be avoided?	Decision Makers
SAP-5	What are the security risks, challenges, impacts and implications of this technology?	System admins



### **3 Migration Plan**

The Collaborative Engineering Demonstrator will attempt to address the above key questions by demonstrating the integrated TrustCoM reference implementation in a realistic business setting.

The scenario will also show how a pool of services and capabilities can be made available by businesses and used to quickly support collaborations.

#### **3.1 CE Demonstrator Requirements**

From the key questions identified in the previous section, the following requirements of the Demonstrator are derived. These requirements are linked with the associated key question where possible. The requirements include functional requirements (ie, requirements for extending existing components or new components), the kinds of experiments and trials to be conducted, etc, etc.

<b>ID</b>	<b>Description</b>	<b>Key Questions</b>
R0	The demonstrator shall be based on elements found in enterprises.	All
R1	A model of a VO (referred to as 'VO' below) will be developed to integrate a set of separate, non-trivial, re-usable services together to provide a non-trivial capability to an engineer.	All
R2	The demonstrator shall provide a demonstration of a VO being designed to implement the VO model ('VO'), including the definition of SLAs, collaborative process and all other content required for the GVOA.	BAE-4
R3	The demonstrator shall provide a demonstration of a VO being created from this definition by means of a pool of service providers.	BAE-13, HLRS-4
R4	The demonstrator shall provide a demonstration of a VO reacting to deal with service exceptions, including selective notification of organisational roles such as legal and financial specialists	BAE-9, BAE-12
R5	The demonstrator shall provide a demonstration of a service provider being replaced due to SLA violations	BAE-9
R6	Web based administration consoles will be developed for selected TrustCoM services	BAE-6, BAE-7
R7	A billing service will be developed to mimic a cash transaction between a service provider and its customer. The transaction should be robust and able to cope with failed or dropped connections.	All
R8	The prototype will demonstrate how many of the TrustCoM services can be outsourced to TTPs, requires minimal deployment of TrustCoM services by end users	BAE-3, BAE-1
R9	The demonstrator shall include CFD services adapted from the SimDat project.	BAE-8
R10	The demonstrator shall include the parallel NEC code as a representative parallel application	BAE-8

R11	The demonstrator shall show the flow of encrypted messages between organisations, possibly via intermediaries such as TTPs	BAE-0, HLRS-1
R12	The demonstrator will demonstrate the critical roles of STS, PDP and PEP in securing the messages between domains.	HLRS-1
R13	The demonstration will show how information filtering on outgoing messages can be performed in accordance with a policy.	BAE-0, BAE-13
R14	The demonstration will show how collaborative processes can accommodate private organisational processes.	BAE-5

### 3.2 CE Demonstrator Model

The following diagram shows a crude system model of the Demonstrator.

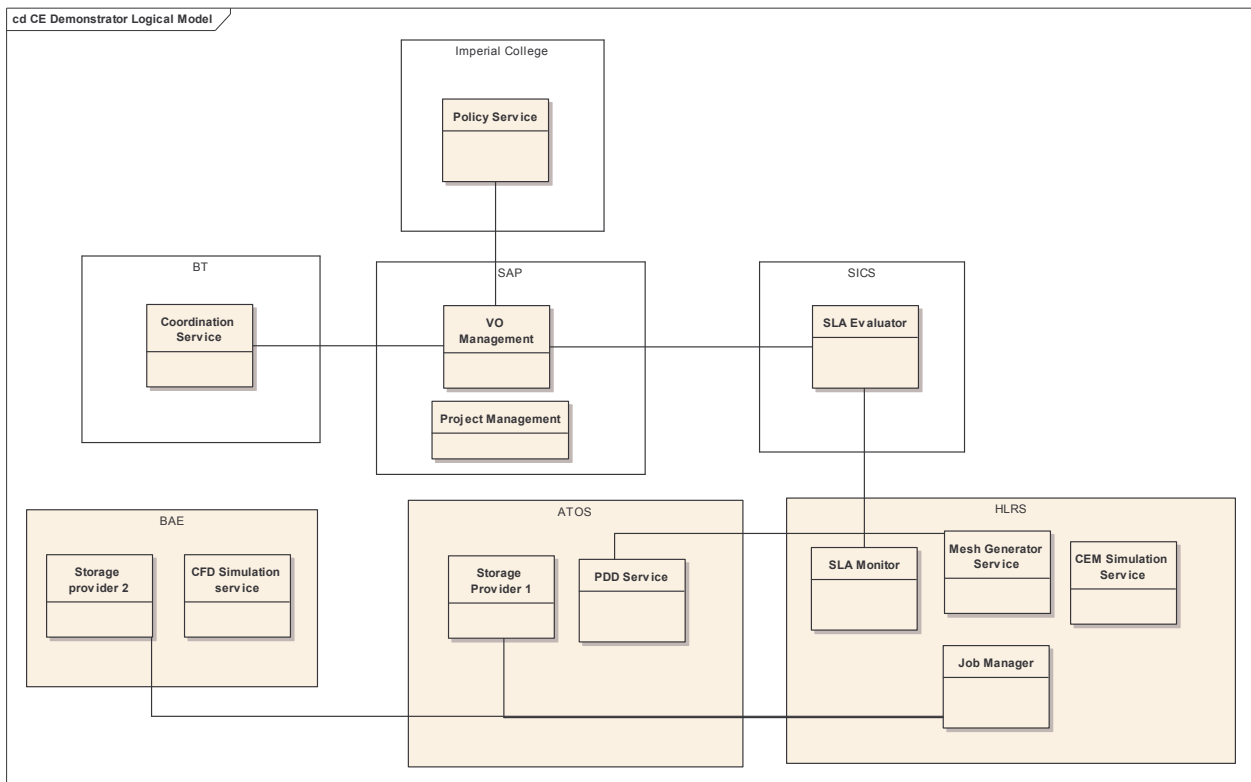


Figure 2 A simplified model of the CE Demonstrator

Due to the limited number of participants, the project partners enact one or more roles, namely, the supporting services role which involves the hosting of a TrustCoM service, or an application service provider role. The former are represented by open rectangles in the figure while the latter are shown with filled rectangles.

It should be noted that BT, Imperial College and SICS are relied on for supporting their respective tools and are not expected to perform any additional tasks within this work package.

Many details have been omitted for clarity, including the PEP, STS and PDP services that support the underlying organisational security. Other supporting services (such as the Secure Audit web service) may be deployed within one of the application service provider domains.

Appendix 7.2 describes one of the possible collaborative business processes planned for the CE Demonstrator. Note that this UML activity diagram describes the collaboration from the point of view of generic business roles, eg, ‘simulation role’, that maps on to more specific business roles such as ‘CFD simulation role’ or ‘CEM simulation role’. Furthermore, there is a strong association between these roles and the application services described in the above figure. For example, the simulation role invokes the Job Manager Service or CFD service shown in the above figure.

### **3.3 Partner Responsibilities**

The following table presents the responsibilities assumed by each partner. A number of partners are directly associated with this work package, while others provide the support to their project contributions developed within AL2.

<b>Partner</b>	<b>Responsibilities</b>	<b>Role</b>
BAE SYSTEMS	WP Lead, provision of application services and data, definition of scenarios, exploitation and dissemination. Hosts application services.	WP Member
UoK	Provision and support for Reputation and SAWS services	App support
IC	Provision and support for scenario policies and policy services	App support
Atos Origin	Support for, and extensions of, Storage Provider and PDD services; dissemination via other initiatives.	WP Member
SAP	VO Management extensions and support. Disseminations through other initiatives and projects.	WP Member
SICS	Provision and support for SLA Evaluation services	App support
HLRS	Hosts parallel NEC Application service; exploitation and dissemination; host of other applications (mesh generator)	WP Member

### **3.4 TrustCoM Components and Prioritisation Issues**

The following table describes the TrustCoM components to be used in the Demonstrator along with comments on their respective roles. Rows are colour coded in line with the adopted colour convention for the TrustCoM Sub-systems (as defined in Appendix 7.1).

<b>ID</b>	<b>Component</b>	<b>Comments</b>	<b>Criticality</b>
CO-1	Policy Enforcement Point	Enforcement of security policies- access decisions, message encryption etc	High

## D37 – Migration and Demonstration Plan

TRUSTCOM – 01945 02/08/2006

CO-2	Service instantiator	For instantiating and configuring the application services when they enter the VO	Medium
CO-3	Coordination Service	For defining a security context that links the simulation/HPC, PDD, Storage provider, mesh generator application services together into a single security context.	Medium
CO-4	Notification Proxy	For notification of events within the VO, eg, changes in reputation value.	High
CO-5	Policy Decision Point	Access control decisions based on security roles	High
CO-6	Policy Service	For storing and executing event-condition-action policies. Also administers policies across the demonstrator.	High
CO-7	Reputation Service	For reporting and disseminating reputation values of the application services- HPC/simulation etc.	Low
CO-8	Secure Audit Web Service	For recording application messages in a secure, traceable environment	Low
CO-9	Security Token Service	Provides Truth assertions from an organisation specifying requestor's security role	High
CO-10	VO Membership Mgmt	For enrolling into or replacing service providers, eg, providers of HPC services, within this VO	Low
CO-11	VO Lifecycle Mgmt	For overseeing the formation, negotiation, operational phases of the VO composed of the services.	Low
CO-12	GVOA Manager	Manages the creation and registration of the GVOA document for the VO.	Low
CO-13	SLA Template Registry	A registry of templates	Low
CO-14	SLA Evaluator	Computes the SLA parameters from the host data	Medium
CO-15	SLA Monitor	Compares the SLA parameters with the agreed SLA	Medium
CO-14	SLA Manager Service	The outward facing interface to an organisations SLA sub-system. Protects the internal sensitive details of the organisations	Medium
CO-15	Collaborative Business Process Management	For overseeing the execution of the collaborative business process.	Medium

We have classified the components according to a criticality level that expresses their importance within the demonstrator.

**High:** very critical for providing the baseline requirements for the demonstrator

**Medium:** critical, but may be replaced with make-shift solutions

**Low:** demonstrator could be re-structured with minimal impact

Given that resources may be limited in the support phase, a prioritisation of the work for these components is necessary. In accordance with the priorities highlighted earlier, the following priorities for components are:

**High priority:** flexible security- a must-have

**Medium:** service quality assurance- SLA related components

**Low priority:** automated management- lifecycle and membership management

All Security components require very highest priority and if any faults were identified then these (or any heavily dependent component) would require the greatest attention. However, in the event of problems with the Coordination service then we will adopt partner-to-partner security relationships instead of a shared security context.

SLA is considered medium priority at present. Service reliability- monitoring of performance and comparison against agreements- is considered to be the most important after security. The minimum SLA requirement here is that the monitoring and evaluation capabilities are correctly functioning.

The VO membership management and other higher-management components such as collaborative business process management are the most ambitious and therefore riskiest to consider. In line with near term objectives for BAE, namely obtaining security and reliability assurance, this will be given lower priority and the demonstrator revised to accommodate any shortfalls in capability that are encountered.

It should be borne in mind that best efforts will be made to demonstrate as many capabilities as possible, including the VO management aspects.

### **3.5 Plan**

In accordance with the revised timescales for the project, it is envisaged that effort on the industrial demonstrator will gradually increase during 2006 as results from the technology phase become more mature, the technologies are better understood and have been validated. Therefore, the remainder of 2006 will be mainly involved with planning, design and extension of current application services, the installation of parallel NEC code, model development and other tasks that have no direct dependency on ongoing framework development. The major part of the implementation phase will begin in 2007 when the final form of the Reference Implementation will be available.

The overall plan includes the following activities:

Activities	Description	Partners	Date
A1	Installation of parallel NEC code at HLRS; model development, deployment of GRIA CFD services	BAE	Commences 08/06
A2	Approval of migration and demonstration plan by reviewers.	All	10/06
A3	Refine list of key questions that would be of concern to the	All	10/06

## D37 – Migration and Demonstration Plan

TRUSTCOM – 01945 02/08/2006

	separate communities of interest of the partners		
A4	Assess results of updated TrustCoM assessment done in AL2- expected to be available October 2006- assess suitability of TrustCoM sub-systems and services for the Demonstrator; modify demonstrator if necessary;	All	10/06
A5	Refine the design of the CE Demonstrator based on the existing CE Test Bed, including a final scenario definition, VO structure and policies and agreements for the GVOA;	All	11/06
A6	Adapt and enhance existing CE Test Bed application services to address key questions posed in Section 2.3	BAE Atos HLRS	12/06
A7	Develop a small set of new application services suitable for 'business-focussed-applications'- eg, billing services- that enhance the demonstrator; introduce transaction support.	BAE Atos	01/07
A8	Introduce more 'user-friendly' interfaces to TrustCoM services if necessary, and with the co-operation of technology owners (eg, of VO Mgmt, etc, etc)	SAP	02/07
A9	Develop client applications, eg, web applications, macros to MS EXCEL, to show the reporting of information from VO Mgmt. Start selected number of experiments described below.	SAP	03/07
A10	demonstrate to WP37 team partners' COIs	All	04/07
A11	report results to the TrustCoM Project and COIs	All	05/07

### 3.6 Experiments

The precise experiments to be designed will be defined within an activity of the migration process, in particular following interviews and discussions with interested parties- including product teams, internal customers and external collaborators in new or existing projects.

The following table shows the current ideas of the experiments to be performed during the demonstration phase. These will be further discussed with the COIs.

ID	Name	Description	Leaders
E1	Definition of GVOA	Demonstration of tools for defining the VO-business roles, choreography, VO policies etc. Aim to show how TrustCoM can enable customers to set up and define a VO easily. Will also identify the current shortfalls and where substantial technical expertise is required.	BAE
E2	Membership negotiation	Demonstrate the selection of HPC providers for membership of VO on the basis of their reputation.	HLRS
E3	Collaborative	Show how public and private internal processes	SAP

	business process execution	can be accommodated within a VO.	
E4	VO Evolution	Demonstrate how poorly performing members can be replaced	HLRS
E5	VO Security	Demonstrate how federated security is managed over the whole lifecycle. Demonstrate the use of policies.	BAE
E6	Message filtering	A demonstration of how basic message filtering can be controlled using a policy.	BAE

This table will be updated following the first evaluation of TrustCoM in AL2.

### **3.7 Risks**

As described earlier, the results of the evaluation exercise in AL2 will be critically assessed for this work package. This will precisely identify the risks involved with the final adoption of TrustCoM components for the demonstrator. If necessary, the plan for the demonstrator will be revised.

### **3.8 Legal Issues**

There are no known legal issues (ie 'issue' as in 'problem') that we can identify at this time. However, some current working assumptions are:

1. We have full access to other TrustCoM technologies in binary form: we do not expect that source code access is required so long as the relevant partner can provide support.
2. Certain applications provided by BAE that were developed outside TrustCoM will have to be licensed and possibly restricted from deployment on the open Internet.
3. Any applications developed outside of TrustCoM that are contributed by BAE will be time-limited to the period of the demonstrator.
4. Confidentiality and non-disclosure agreements may need to be entered into by some partners if further interest in the technologies is initiated. For example, a product team within a company may need to disclose some information to the Demonstration team so that the team can provide advice on how TrustCoM would benefit their products. These discussions may be bound by some kind of NDA.

## **4 Demonstration and Reporting Plan**

This section describes what we will demonstrated by particular partners to their particular communities of interest and how it will be reported.

### **4.1 BAE Demonstration and Reporting Plan**

For BAE SYSTEMS, there is interest in being able to exploit our in-house capabilities in CFD, CEM and CSM to an external market as accessible web services. These services could participate in engineering Virtual Organisations that include industrial and academic partners. The range of possible collaborations include:

1. national, local and European projects in civil application areas- environmental, industrial
2. European and other international Joint Ventures, focussed at sharing capabilities

The resulting CE Demonstrator will be shown to internal customers (within corporate IT) and external collaborators (including Airbus UK and EXOSTAR) as significant results are achieved. For corporate IT, the main interest is currently in federated security. For EXOSTAR, the possible opportunities from having a web service based supplier base.

In the military sector, the demonstration of federated security, policy based systems and business process management systems will be of interest. Therefore, sub-demos of the CE Test Bed will emphasise how TrustCoM's federated security and policy systems can be used to share information and asset data between decision makers in military collaborations. This will show potential customers how the tools could be exploited and prompt further interest in the framework from this community.

Recommendations from an end-user point of view will be provided in deliverable D56.

Major collaborative engineering events during the lifetime of TrustCoM (first half of 2007 when the demonstration will be more mature) will be identified

### **4.2 HLRS Demonstration and Reporting Plan**

HPC resource provisioning is coupled with high demands in the areas of security standards (access restriction, data protection and user authentication), as well as administration and maintenance (incl. management of the resources and jobs). In addition, some HPC providers will restrict their resources regarding the customer's trustworthiness on basis of a *negative* recommendation system, i.e. whenever the customer was judged untrustworthy by some other, well-known party.

Accordingly, HLRS will demonstrate the capabilities of the TrustCoM framework in the context of High Performance Computing resource provisioning: the University of



Stuttgart currently provides HPC to a series of automotive, government, SME engineering companies and academics that make use of the environment for their respective complex calculations. Each user puts forward different demands to the system according to their respective needs and budget. Along the same line, not only the required quality of service parameters differ widely, but also - implicitly - the pricing for these services.

TrustCoM will allow resource consumers easy deployment and execution of their calculation jobs by autonomously supporting access right restrictions, as well as authentication, security enactment and reputation management. At the same time, TrustCoM will reduce management overhead by supporting Service Level Agreements specifying the individual cost terms and usage conditions thus giving the resource provider a means to autonomously supervise his resources. This reduction in overhead will allow easier maintenance of the resources and thus cheaper services for business customers.

### **4.3 SAP Demonstration and Reporting Plan**

SAP will use the demonstrator to influence their software products by using it as a demonstrator within the company and for potential customers. It will show how to manage VOs in an integrated fashion as a business concept in B2B scenarios that minimizes the administration overhead without unnecessarily sacrificing security.

### **4.4 Reporting Feedback**

#### 4.4.1 Technology Level

The following table will be used to express the findings of the experiments and demonstrations of the TrustCoM Reference framework for the various planned experiments. Criteria will be based on those developed within AL2 evaluations [6].

<b>Technology Level</b>	<b>Description</b>
TL-1	Proof-of-concept
TL-2	Fit for demonstration within a limited business-type scenario
TL-3	Fit for prototype field trials with extensive user support
TL-4	Fit for general release as an open source toolkit

The rating will be applied across the integrated framework and over the different phases of the VO life-cycle:

<b>Life-cycle Phase</b>	<b>Scenario context</b>
Identification	Design of collaborative engineering process; SLA requirements; security policy definitions

## D37 – Migration and Demonstration Plan

TRUSTCOM – 01945 02/08/2006

Formation	Identification of required app services (CFD, CEM) from pool of service providers;
Operation/Evolution	Removal of poorly performing service providers; replacement by new service providers
Dissolution	Clean termination of VO.

The criteria for deciding the Technology Level of the system is being developed as part of WP35 [6].

We will make recommendations for moving to the next TL. Eg, if it is found that the Definition phase is TL-2, we will make recommendations for improvements that will move it to TL-3.

## **4.5 Contribution to other initiatives**

Each partner will endeavour to promote the demonstrator through other regional, national and international projects and initiatives. These are intended to satisfy the third objective, ie, the re-use of TrustCoM results within other projects and initiatives.

<b>Partner</b>	<b>Initiatives</b>	<b>Strategy</b>	<b>Timescales</b>
BAE SYSTEMS	SimDat (Euro)	Demonstrate application of SimDat application services within TrustCoM framework, where possible. Promote architecture and profiles.	2006-2007
	CFMS (UK)	Centre for Fluid Mechanics Simulation. Demonstrate how TrustCoM can improve the management of services within aerospace collaborations.	2007-
	CRISP(UK)	Re-use TrustCoM framework as a candidate architecture for CRISP.	2006-2008
HLRS	Initiatives related to HPC European projects	Exploit TrustCoM concepts and technologies that may benefit next generation Grid projects in Europe and regionally.	2006-
Atos	NESSI	Identify tools suitable for further exploitation in NESSI, identify capability gaps and requirements for future NESSI related projects.	2006-
SAP	XtreemOS (Euro)	Port elements of VO management to the application level of a prototype Grid platform for Business	2007 – 2009
	SAP Internal	Transfer the knowledge gained from security and VO management in TrustCoM to development in the area of B2B and Web Services	2006 – 2008

## **5 Conclusions**

The demonstrator will attempt to show the business benefits from using the TrustCoM framework while at the same time demonstrate how the reference implementation addresses concerns over security, reliability and manageability issues that arise from participating in collaborations.

The demonstrator will be used to influence and shape the post-TrustCoM development and employment of TrustCoM results by attracting the interest of a) potential customers and service providers, b) IT managers, c) commercial software vendors. If the reference implementation of TrustCoM is to have a future as an open source project then it needs to have some tangible demonstration of its capabilities and the advantages it brings to service-based collaborations.

The demonstrations will also provide final evaluations, giving some steer for the development of future editions of TrustCoM.


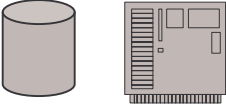
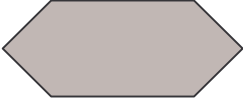
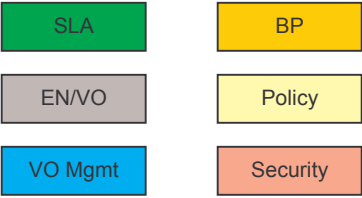
## **6 References**

1. Baseline Prototype Infrastructure for the CE Scenario, TrustCoM deliverable D10.
2. Revised TrustCoM Reference Architecture, TrustCoM deliverable D62
3. Revised TrustCoM Reference Implementation, TrustCoM deliverable D53
4. Requirements for the Collaborative Engineering Test Bed, Internal TrustCoM deliverable ID2.2.1
5. SIMDAT Project home page. <http://www.scai.fraunhofer.de/710.0.html>
6. Enhanced CE Test Bed, TrustCoM deliverable D41.



## 7 Appendices

### 7.1 Symbols Used in the Text

Symbol	Description
	A web service component
	Resources such as file storage, HPC servers etc.
	A software component such as an API or software artefact that supports a service.
	TrustCoM sub-systems for SLA management, VO management, Business Process Enactment, Enterprise Network/VO Infrastructure, Policy and Trust and Security.

## 7.2 Appendix 1: CE Demonstrator Collaborative Business Processes

The following diagram shows the roles and interactions involved with a typical collaborative engineering analysis/simulation process in the CE Demonstrator.

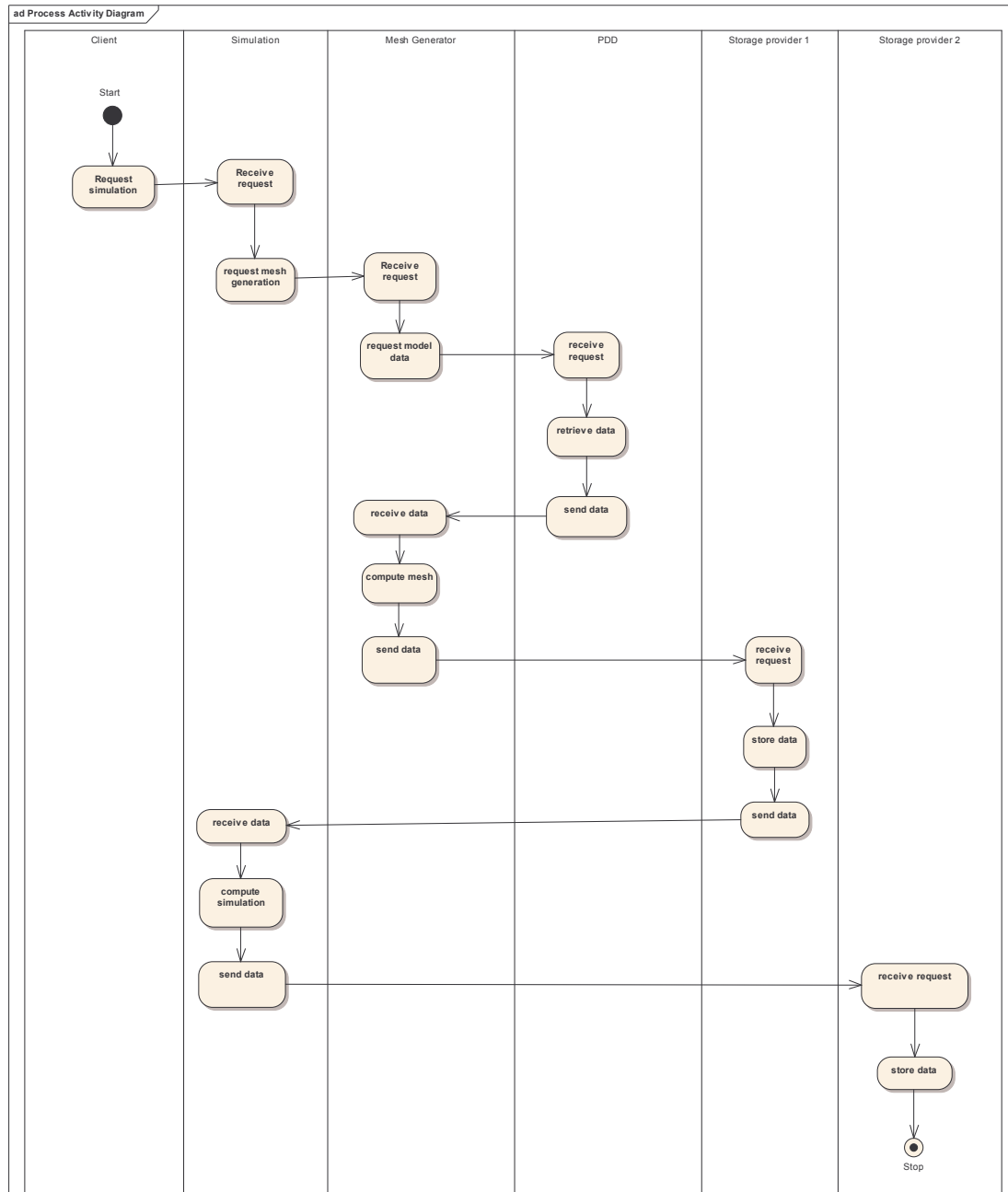


Figure 3 CE Demonstrator collaborative business process

The collaborative business process involves new engineering roles:

**PDD**: retrieves engineering design data from a database



**Mesh generation**: required for computing simulation meshes from the input design

**Simulation**: for computing simulation data from the mesh data

Note that the mesh data produced by the mesh generator is stored on the 'storage provider 1' service for quality reasons so that it can be retrieved in possible audit procedures. This data is then used in the simulation process role for performing the calculations of, for example, a flow field. The output results are stored to another storage provider that has extra facilities (not shown here) for data mining and extraction.

Simulation processes considered within the test bed include:

1. electromagnetic simulation of the panel antenna on the aircraft, and
2. fluid dynamic simulation of the aircraft.

Other services that may be involved here are not shown for clarity reasons. These include the bank service for example, where the bank account of a customer of a service is debited at the end of the simulation.