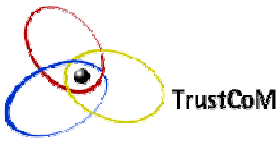

Deliverable

D69

Final Implementation and Validation of the Collaborative Engineering Demonstrator

WP37 **Collaborative Engineering Demonstrator**

David Golby Editor

BAE SYSTEMS Advanced Technology Centre

6th June 2007

V1.0

Contributors

Lutz Schubert (HLRS)

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 2007 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.

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: AL3 Demonstration Trials

Activity: Activity 3.1 Collaborative Engineering Demonstrator

Work Package: WP37 Collaborative Engineering Demonstrator

Document title: Final Implementation and Validation of the Collaborative Engineering Demonstrator

Version: v1.0

Document reference:

Official delivery date: 31st May 2007

Actual publication date: 6th June 2007

File name: D69 Final Implementation and Validation.doc

Type of document: Report

Nature: Public

Authors: David Golby (Editor)

Contributors: Lutz Schubert (HLRS)

Reviewers:

TABLE OF CONTENTS

Version History **8**
Executive Summary **9**
1 Introduction and Background **11**
1.1 TrustCoM Project background **11**
1.2 Relationship to the CE Test Bed **11**
1.3 Goals and Objectives of the Final Phase **12**
2 Description of Final Demonstrator **13**
2.1 Business Model **13**
2.1.1 Drivers and Incentives for SOA 13
2.1.2 CE Demonstrator Business Model 15
2.2 Application Scenario Outline **15**
2.3 VO Lifecycle Description **18**
2.3.1 Discovery Phase 18
2.3.2 Negotiation and Configuration Phase 19
2.3.3 Operational Phase 19
2.3.4 Evolution 19
2.4 Implementation **21**
2.4.1 Demonstrator Architecture 21
2.4.2 Development of the Decifer Client 22
2.4.3 Development of the Decifer Partner service 23
2.4.4 TrustCoM Deployment Tasks 25
2.4.5 TrustCoM Components Used 27
2.4.6 Components used from the CE Test Bed 27
2.4.7 Background Material 27
2.4.8 Demonstration Deployment Model 29
3 Application View of the CE Demonstrator **30**
4 Business Benefits **33**
4.1 Introduction **33**
4.2 Current Practices for Collaborative Design **33**
4.3 Improvements to CE using TrustCoM **37**

4.3.1 Technical Benefits 37
4.3.2 Business Benefits 38
4.4 Improvements in other Product Lifecycle Phases 40
4.4.1 Manufacturing 40
4.4.2 Product Support 41
5 Future Work 43
5.1 Near Term Objectives 43
5.1.1 Infoset Generation 43
5.1.2 Discovery Phase 44
5.1.3 Formation Phase 44
5.1.4 Operational Phase 45
5.1.5 Dissolution Phase 47
5.2 Long Term Objectives 47
6 Conclusions 49
7 References 52
8 Appendices 54
8.1 Appendix 1: Preparation Phase Information 54
8.1.1 STS Configuration 54
8.1.2 XACML Control Policies 55
8.2 Appendix 2: CE Demonstrator Architecture and Deployment Details 56
8.2.1 Top-level View 56
8.2.2 Gateway Sub-system- Interaction View 57
8.3 Appendix 3: Collaborative business process: detailed view 59
8.4 Appendix 4: Installation and Configuration of the Gateway 61
8.4.1 Generating and Installing the certificates for the STS. 62

Glossary

An explanation of terms used within the document.

Term	Description
ACL	Access Control List.
BPE	Business Process Enactment- the business process management sub-system in the TrustCoM framework.
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.
CE	Collaborative Engineering
CEM	Computational Electromagnetic Modelling. The modelling of radar, antenna performance (mobile phones, aerials, radio etc) by means of numerical techniques similar to CFD.
CFD	Computational Fluid Dynamics. The use of computers for the simulation of fluid (eg, air, water) behaviour. Used in weather forecasting, aerodynamics etc.
COI	Community of Interest. A particular interest group such as customers, system administrators, application developers, middleware providers etc etc.
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.
QoS	Quality of Service.
SLA	Service Level Agreement. The electronic agreement between the service provider and customer.

SME	Small to Medium Enterprise.
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.
TrustCoM RI	TrustCom Reference Implementation. The set of applications and services that implement the TrustCoM Architectural Framework.
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.
TTP	Trusted Third Party.
VO	Virtual Organisation. A model of a collaboration that involves companies, academic institutions, governmental organisations sharing resources to achieve a common objective.

Version History

Date	Description	Subversion Revision Id
01/02/07	Skeletal outline of the document	6955
06/06/07	Final Version	Latest version

Executive Summary

The work reported here describes the final implementation phase of the TrustCoM CE Demonstrator. The major part of the development was completed following the final release of the TrustCoM Reference Implementation in Feb 2007. As a result of this late delivery, work has had to focus on key aspects of security, performance and VO management.

During this period more realistic application services have been used within the TrustCoM framework for the first time by the TrustCoM CE team. Some challenges were encountered in doing this but these were overcome with a solution that was pragmatic and consistent with the principals of the TrustCoM framework. The collaborative business process model, security policies, SLAs and Event Condition Action policies that have been used in the work has been based on the documents developed during WP35 for the CE Test Bed. Other components such as the Storage Provider service that were developed for the CE Test Bed were re-used for the CE Demonstrator. In summary, the CE Demonstrator shares many superficial similarities to the CE Test bed but with more challenging applications involved.

The demonstrator meets the basic requirements for security and performance monitoring. Partners' resources can be protected and are only accessible to other partners in the VO. Messages can be protected in transit from interference and inspection from other external parties. This is the most important risk that needs to be addressed before collaborations on an Open Internet can be considered. A facility for comparing the service performance with agreed metrics and performance targets is provided and this is sufficiently flexible for supporting either reserved CPU or storage requirements- two common requirements for CE.

The formation and operation of the VO is facilitated by use of the VO Toolkit. A VO Initiator can specify the basic VO roles and their interactions (via a pre-defined CDL document), the required security policies and the required policies for managing and taking corrective actions to protect the operation of the VO. Some limited management capability has been demonstrated that shows how certain risks- such as partners defaulting on their agreement- can be contained and managed. The system is flexible enough for different policies to be deployed for managing these exceptional events in the VO.

The demonstrator is a significant improvement over current online collaboration solutions. These tend to be portal based, slow and prevent the required application integration that can automate performance-critical applications, such as for design-optimisation. Adopting an SOA for integrating applications within an engineering collaboration significantly improves this situation but does not by itself address all the requirements for security, performance and management that need to be addressed for online application sharing with (initially) unknown partners. TrustCoM provides certain solutions in these areas that significantly reduces the threats of a) security threats, b) uncertain performance of partners, c) management complexity that arise from using SOA over an un-trusted network.

The business benefits that arise are identified to be in risk reduction through application of a scalable security model that is suitable for on-line collaboration of enterprises. Management costs and overheads are reduced through use of federated security, enabling organisations to share resources without explicit registration of a partner's operatives. This also improves time-to-market as well. Further management costs are achieved through autonomous monitoring of service provider performance and limited autonomous management of their effects. Entry level times are potentially reduced via use of the VO Discovery service, where partner reputation provides some assurance (if it this reputation metric is trusted itself of course) that a new partner has the best relative business competency out of a set of unknown providers. Finally, a business agreement is generated that integrates the required technical requirements- security, performance- with other terms and conditions that typically prevail over the partnership. This can be viewed and agreed by all parties before the VO begins.

However, further work is required for making the aforementioned policies and agreements easier to compose and negotiate. It is recommended that further work be pursued in providing tools that support the easier composition of policies (ECA, XACML), performance agreements (SLA), consortium agreement (GVOA) and collaborative business process (CDL) documents. The ability to easily compose these documents would lead to a reduction in the technical skills that are currently required for creating or changing these documents. This is regarded as the most significant factor that would need to be improved before the demonstrator became an acceptable proposition for on-line business.

1 Introduction and Background

This document describes the final development phase of the CE Demonstrator. This includes a description of the technical work done and a validation of the TrustCoM framework in the context of a Collaborative Engineering scenario.

The term 'validation' needs to be treated with care in this context. By validation is meant an assessment of business benefits from using TrustCoM to the particular business scenario that has been used in this study. A more detailed *technical* evaluation of the TrustCoM framework that looks at functional and more 'lower-level' aspects of validation is described in the final Evaluation report [5].

This section presents an introduction to the document setting out the background to the final phase of work. It describes the circumstances of the work and the goals and objectives that were defined for the final phase.

1.1 TrustCoM Project background

The final phase of the R+T project action line in TrustCoM was completed late, with a final TrustCoM Reference Implementation delivered in Feb 2007. It was only in the period since the March TrustCoM Review that the Demonstrator team have been able to use a version of the RI that is sufficiently mature and stable for completing the demonstrator and to assess its overall capabilities.

1.2 Relationship to the CE Test Bed

The CE Test Bed [4] was intended for specifying requirements for the TrustCoM framework and to incorporate software components that were easy to install at other partner sites. The applications were not intended to be robust or to an industrial standard- these typically have requirements for HPC platforms that are not generally available among the project membership. Furthermore, licensing restrictions would have prevented in-house BAE applications from being deployed on other partner's systems that were connected to the open Internet. Therefore, the applications chosen for AL2 were intended to be generic examples of typical engineering services used for Grid research and engineering collaborative projects and fit for the software development phase of TrustCoM.

In the CE Demonstrator, more realistic engineering applications are deployed for the first time. It should be noted, however, that much of the work done in the CE Test Bed has been re-used for the Demonstrator. It has re-used the general design principles learned in the CE Test Bed and adapted results such as the CE Test Bed choreography, access control policies and security federation data as well. The main application components share many similarities and behaviours. For example, the evaluator service used for the optimisation process has a similar interface and behaviour to the NEC antenna service. Other CE Test Bed components such as the

Storage Provider service have been adapted with some minor extensions for this study.

1.3 Goals and Objectives of the Final Phase

The objectives of the final phase are:

1. to complete the application services reported in the previous deliverable
2. to complete the integration of third party components- specifically GRIA- into the Demonstrator
3. to demonstrate the most mature and promising aspects of the TrustCoM RI using these application services
4. to use real-life engineering applications that would be of relevance to clients of the ATC team
5. to assess the technical capabilities of the TrustCoM RI.
6. to assess the business benefits from using TrustCoM as compared to traditional online collaborations.

2 Description of Final Demonstrator

In this section, a detailed description of the demonstrator is given. The first section gives a top-level view of the application scenario.

2.1 Business Model

This section describes the Business Model view of the CE Demonstrator, indicating some of the motivations for the work from BAE and HLRS perspectives.

2.1.1 Drivers and Incentives for SOA

The drivers for the adopting SOA for Collaborative Engineering come from three different sources:

1. the need to form collaborations where best capabilities (applications, data) are shared within an engineering joint venture;
2. the need to reduce internal administration and capital costs through the outsourcing of IT Services to external providers.
3. future business opportunities for deploying in-house numerical simulation services in partnership with HPC providers

2.1.1.1 Sharing capabilities within Joint Ventures

In the first case, companies specialising in particular engineering capabilities (eg, airframes, avionics and control system software) need to work together throughout the whole product lifecycle. If a new concept or idea is being developed, then the design phase is very critical for identifying and eliminating any risks that may appear later in the product lifecycle. The design teams in each company will typically have their own applications and solutions that have been targeted at a specific sector. The requirements here are that applications and data will need to be integrated between these design teams into a set of 'super applications' that can be used together to improve the design. Current practice may involve creating new infrastructure and facilities to serve the partnership- eg, trusted third parties that can host web portals. Other solutions would involve drawing up licensing agreements to protect the application being shared. However, these measures may be expensive to implement or disruptive to the internal systems used by each partnership, particularly if it is short-lived. Furthermore, this kind of integration must be done in such a way as to ensure that the owner retains control and ownership of his particular capability. Sharing these capabilities as services is an attractive option though there would be concerns about security- of data and systems- that would need to be addressed.

Why TrustCoM? TrustCoM offers solutions to security and manageability that may address the security requirements of the partnership described here. The TrustCoM

Federated VO security model offers the ability to share web services between two engineering organisations without any expensive integration of identity management systems. Furthermore, it offers the ability to control access to web services by means of access control policies.

SLA and VO Management would not be critical factors here. The collaboration would be static and would not be expected to change frequently. A collaborative business process may be used to precisely define interactions between the partners, but all other TrustCoM components such as SLA monitoring would not be necessary. Finally, a GVOA would not be necessary as an existing traditional collaboration agreement would already be in place.

2.1.1.2 IT Outsourcing

The second motivation reflects the trend for outsourcing resources to external providers. Within many enterprises, both large and small, IT services are outsourced to a single contractor. This arrangement has the advantage of reducing internal administration costs and freeing resources within the client company to focus on core capabilities. From the service provider's perspective, many different sectors could be serviced from the same set of capabilities and facilities. This is particularly the case for storage and HPC provision, where the basic requirements are technically similar for many different markets.

However, business requirements may change and corresponding IT requirements may have difficulties catching up. For example, demand for HPC resources in an engineering company may rise and fall depending on the state of its current and future programs. Furthermore, a single provider may not provide all of the services that the company requires and so a number of different providers would be required. Using more than one provider, however, may be difficult to manage and may lead to increases in supply management costs.

Why TrustCoM? TrustCoM's SLA Management model would now be a critical supporting component that would help to realise this business scenario. This would ensure that a client and service provider would have mutually agreed performance indicators captured within a machine-readable document that could be used to monitor performance and compare it with agreed performance requirements.

2.1.1.3 Software as Services

The third scenario involves offering a software service on an open market of engineering service providers. It is the most direct opportunity for business revenue for a company such as BAE in any future exploitation of SOA on an open market. In this scenario BAE, in collaboration with other partners, would provide a novel engineering-design capability to a customer. For example, an engineer in a small company who does not have the in-house resources to run large scale optimisation calculations could use the capabilities of an optimisation VO to improve the performance of his product design. The VO formed by BAE and other partners would then offer this service on a pay-per-use or subscription basis.

Why TrustCoM? This scenario offers the most comprehensive application of the TrustCoM RI. The VO security model would ensure that services within the partnership would be protected from external parties, while the SLA sub-system would ensure that agreed service levels within the partnership would be maintained. This is a critical requirement of the HPC and the storage provider service. If the HPC partner defaulted on its SLA then it would be in breach of the partnership agreement and would be subject to penalties or even replacement within the partnership by an alternative provider. The VO Management system becomes a critical additional requirement here.

2.1.2 CE Demonstrator Business Model

The business model to be pursued in the CE Demonstrator uses elements of all three business drivers described earlier. It comprises actors who provide commodity services that are critical to an engineering VO. Their performance is critical to the success of the VO.

2.2 Application Scenario Outline

The following diagram shows a top-level view of the actors in the collaboration.

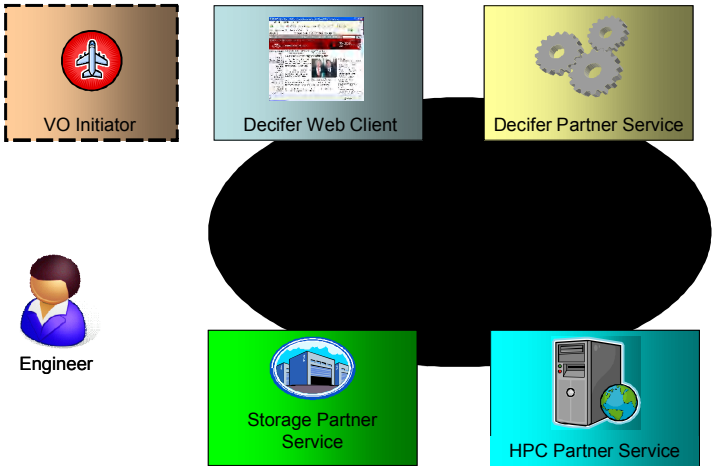

Figure 1 CE Demonstrator Scenario Top Level View

The application scenario is as follows. An aerospace company is a prime contractor within some major aerospace project that is engaged with developing medium range civil aircraft. Due to environmental regulations and rising fuel costs the aircraft has to have low emissions and have efficient fuel consumption. At the time of this scenario the project is in the design phase and there is a need to have a range of advanced design tools that can help to improve the design to meet the product performance requirements. Furthermore, these applications need to be shared between the prime contractors and their suppliers.

Therefore, to meet this need the prime contractor decides to put together a new mini-consortium of smaller companies that overall delivers a range of design/analysis capabilities that are required. One of these- a design-optimisation service- is the one of particular interest within this scenario.

The VO is intended to be composed from services provided by a number of actors, all of which are to work together to deliver the required effect. The first of these is a web portal provider that hosts an industry-standard product design database. The second actor provides the design-optimisation algorithms that must be used for exploring in a fast and efficient way the many design-options that need to be generated and compared against the performance requirements of the product being designed. This service in turn requires high performance computing facilities to explore these design spaces by executing numerical simulations for each individual design. Finally, the results of the optimisation need to be stored in a highly secure facility that is suitable for storing industrial engineering analysis data for long periods of time. This VO is at this point of time an abstract specification or 'wish-list' of services that are required to work together.

The VO that is formed from these requirements comprises the following members: a) an aerospace company that provides an engineering web portal ("Decifer Client"); b) a scientific/engineering consultancy that has developed an advanced optimisation capability for a niche market- specifically for aerospace design work ("Decifer Partner Service"), c) a HPC service provider ("HPC Partner Service") and d) a storage provider ("HPC Partner Service"). These partners comprise the 'Optimisation VO' shown in Figure 1. The prime contractor is in TrustCoM terminology the VO Initiator who has an operative who specifies the VO.

As noted earlier, certain of these roles can be described as 'basic commodities', such as the HPC and specialist storage provider partners. The HPC providers serve a wide market, including animation, image processing and engineering/scientific numerical simulations. By contrast, the storage providers are specialised to sectors that have high security and maintenance requirements associated with large volumes of engineering and scientific data. Given the commonality of these requirements, the service supports a wide range of technical manufacturing sectors (aerospace, automotive, etc). In short, the market model is that of a number of highly competitive providers who serve a wide number of sectors.

The following diagram shows a top-level representation of the overall collaborative process that is enacted within the Optimisation VO. This process can be described from two perspectives- the engineer's perspective and from the VO partners' point of view.

3 Application View of the CE Demonstrator

The final TrustCoM evaluation deliverable [5] contains snapshots of the VO Toolkit as it is used for putting together the optimisation VO. These can be considered the precursor steps to the scenario described in this section.

The following screenshots show the client's experience of using the Optimisation VO. As described before, the VO is set up using the VO Toolkit and enters its operational state. It is at this point that the user can start to make use of the new optimisation capability supported by this new VO. He/she is spared the details of the interactions that occur behind the scenes as the collaborative business process progresses.

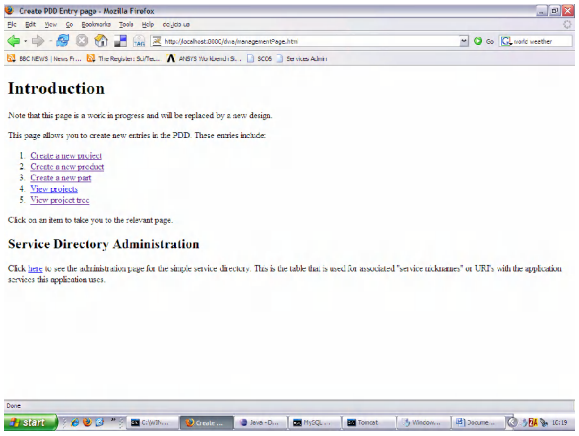

Figure 6 Decifer Web Site Entry Page

The following snapshots show how the user can create a new design project within the PDD. The site is structured into projects, projects are composed of products and products are aggregates of parts. Each part has an associated set of documents-design, analysis, requirements etc. The portal enables the user to navigate to the required design-optimisation document for the given design part using a tree-like navigator.

Figure 9 GRIA job status page showing executing Decifer Job

At the end of the run, the job completes and the output data is written to the storage provider service. The client can visit the site and select the output file for downloading and further processing, eg, to inspect the convergence history information.

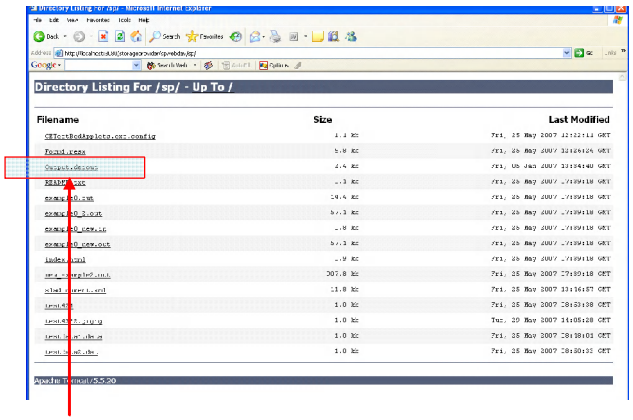

Figure 10 Storage Provider Service

4 Business Benefits

4.1 Introduction

This section discusses the potential business benefits for CE from TrustCoM. It does this by comparing the current practice of collaboration with the solution offered by the CE Demonstrator.

The following section reviews the current practices for forming engineering collaborations and gives indications of performance bottlenecks or 'pain-points' which need to be improved. This is followed by a section that describes the potential improvements in collaborations that may be provided by using TrustCoM technologies.

It should be emphasised that the focus of CE in TrustCoM has always been on the design phase of the product lifecycle. It has not to date directly considered other phases such as manufacturing, product support and product decommissioning. Each of these phases have their own requirements for SOA and are discussed later in this report in Section 4.4, though to a lower level of detail. This is an opportunity to present some preliminary ideas of how the TrustCoM results could be applied to these areas as well.

4.2 Current Practices for Collaborative Design

At this time of writing, BAE SYSTEMS does not use web services to share applications or data within engineering collaborations such as Typhoon, JSF etc. Projects such as TrustCoM, SimDat and the UK-funded project CRISP project are a first foray into this area and are still attempting to win the business case for SOA as an important technology for improving the efficiency of CE.

The current practice for online collaborations is to use a trusted-third party to host a portal provided eg, by EXOSTAR. This is used for sharing project data and co-ordinating document workflows associated with engineering processes. While this solution may have some immediate benefits for many engineering activities, it is obviously somewhat limited for design/analysis activities where applications provided by partners need to be integrated.

Table 4 is a summary of the current ways in which collaborations form over the whole of the collaboration lifecycle when a portal solution is adopted.

In fact, the kind of application scenario envisaged for the CE Demonstrator would be practically impossible or would be extremely limited within this portal-centred collaboration approach. The Decifer Partner service would have to be collocated with the HPC service, requiring complex licensing agreements if the code was very sensitive to the company that owned it. Indeed, the application may not be very portable in the first place and this may limit the scope of the deployment of the

application to a very limited number of HPC partners. One option would be for the whole 'collaboration' to be hosted by a single partner that integrated these capabilities by itself (a), while another would involve the partner interacting with two portals as in (b).

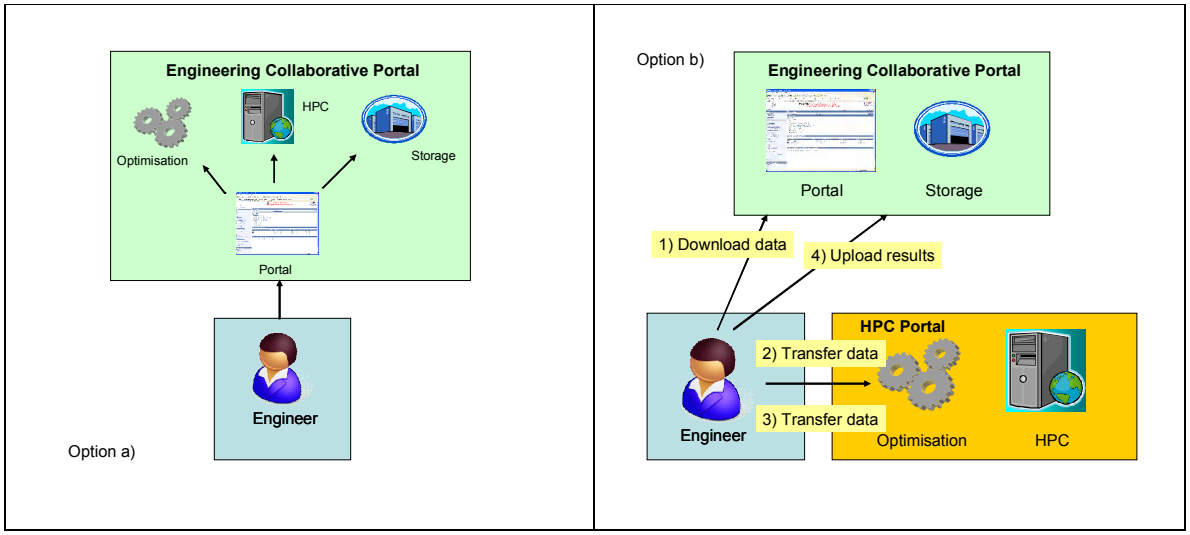

Figure 11 Options for Traditional Engineering Portal Solutions

The first solution would offer the most convenience to the customer, as all of the interactions are managed internally and a simplified interface is given to the user. From the perspective of the portal operator, however, this would require the aggregation of a number of systems and applications that may be beyond his ability to manage.

The second option would be preferable to the portal operator(s) as now individual functions are devolved and can be focussed on individually. However, the business process now critically depends on the end user who would have to act as the 'man-in-the-middle' transferring data between the sites. This process should in fact be automated and would not be appealing to the customer.

Although the second option may be preferable for both portal providers, the HPC portal would still aggregate applications that it would prefer not to host. Other inhibiting factors include software licensing restrictions that may prevent the optimisation service, for example, from being hosted outside the bounds of the company that developed it.

In short, the particular problems encountered in this approach are:

1. many of the processes in forming and managing the collaboration are human oriented and slow
2. discovering new partners with the required competencies is slow

3. bottlenecks such as the data transfer problem for option a) become commonplace and this affects the efficiency of the process.
4. co-ordination of activities and internal processes across the collaboration is not optimal as the portal(s) act as (a) bottleneck(s).
5. the structure of the collaboration is static and cannot be changed without a great deal of effort
6. contract negotiation and formation is paper-based and is slow. It also disjoint from the technical requirements of the collaboration- such as the security policies and service level agreements.
7. a provider would need to host additional capabilities outside the scope of his core competencies
8. integration – or the process of connecting systems or installing and configuring applications – is slow and may inhibit collaborations.
9. software licensing restrictions may prevent certain applications being hosted within partner systems.

Adopting an SOA for integrating applications within an engineering collaboration significantly improves this situation. Applications would be deployed as services instead of portals, expensive user interface development would be avoided and so on. However SOA does not by itself address all the requirements for security, performance and management that need to be addressed for online application sharing with (initially) unknown partners. Instead, SOA should be considered as an important foundation technology for further developments of collaborations through projects such as TrustCoM.

Lifecycle Phase	Security	Contract	Business Process	Business Problems/Risks
Discovery	Partners have different security systems and procedures that need to be taken into account, possibly hindering collaboration.	Risk assessments by each partner include assessing new partners business reputation-based on data from trusted external sources such as business consultancies and standards bodies This process may be slow and the data used of unknown accuracy and out of date.	Discovering the most suitable partners that can meet the required business roles and competencies can be lengthy and time-consuming. Integrating internal activities with the overall project activities may be difficult and could be an inhibitor to collaborative partnerships.	• Researching unknown partners for their business competency is time consuming and costly, increasing the time-to-market • Integrating different security systems may not be possible • Registration of new users to systems is time consuming and costly.
Formation	Individual Security registration required, which is lengthy. Security configuration-policies need to be defined.	There is no common language for defining technical performance requirements. This makes negotiation of terms and metrics slow.	Internal business activities are modified and possibly reconfigured for the collaboration, which may be disruptive to the business.	• Software licensing restrictions may be inhibitors to outsourcing • Security registration presents administrative overheads • Internal business processes may be affected or modified for the sake of a collaboration • SLA negotiation is slow • Cost overheads due to designing and implementing web sites for helping users acting in 'man-in-the-middle' roles.
Operation	Security enforcement is done at the web site at log on time. Messages and activities within the portal may be logged. Security restrictions may prevent easily federated web sites.	Partner monitoring may not be automated. If it is automated, then the performance data may not be easy to interpret within other partners' decision making activities.	Since the human is in the loop, each portal would need a suitable interface that enabled the user to perform his tasks correctly. Data needs to be transferred between portals	• Processes become error prone and slow due to lack of automation • Processes become critically dependent on the 'man-in-the-middle', increasing personnel costs.
Dissolution	Revoking security privileges is not easy to do.	Monitoring systems need to be stopped, increasing administrative overheads	Termination of activities may be difficult to identify if the activities are not formally defined.	• Security administration overheads from reconfiguring systems to pre-collaboration state.

Table 4 Characterisation of Collaborative Engineering- Current Practice using Portal based solutions and the identified business risks

4.3 Improvements to CE using TrustCoM

The following table indicates how the various TrustCoM components could benefit collaborative engineering design for each of the critical areas that have been identified.

4.3.1 Technical Benefits

The VO model provided by TrustCoM provides the following technical benefits:

1. The ability to form protect messages exchanged between partners within the VO
2. A flexible messaging infrastructure that enables services to be deployed once and shared between different collaborations
3. An extensive use of Policy-based administration- access controls, ECA rules etc- that enables the behaviour of security and administrative systems to be changed without starting/stopping them
4. A performance monitoring system that uses electronic agreements to ensure that members conform to their agreed performance targets.
5. An event brokering system that decouples many critical components from each other. This provides greater flexibility in composing and deploying an administrative system that is suitable for the particular application needs of the VO
6. A choreography model that offers advantages over the orchestration model of business processes promoted to date.
7. A management system that facilitates the replacement of erring members within the VO without major disruption to the operation of the VO
8. A system for forming an electronic contract that binds technical obligations – security policies, SLAs, CDL etc- with the legal terms and conditions that need to be abided by all of the partners.

The choreography model used by TrustCoM does not assume there is a central orchestrator or controller that controls all of the activities in the VO. Instead, control is dispersed over the VO so that activities can run asynchronously and in more loosely coupled ways. This ensures that there is no central controller that threatens to become a performance bottleneck during the execution of the collaborative business process. It is also a more natural metaphor for real-life business processes as well.

4.3.2 Business Benefits

In terms of business benefits:

1. a greater degree of automation of the application business process is now possible, improving reliability and reducing administrative costs
2. by adopting a common language of performance requirements, security policies and business definitions, time to market is reduced
3. by using standards for security, messaging etc, interoperability of services is improved and integration costs should be reduced
4. by formalising the roles and duties in a collaborative business process, uncertainties are reduced and risks are minimised.
5. risks in identifying trustworthy partners are reduced through shared reputation values
6. operational risks are reduced through use of precisely defined business models
7. internal business activities- an important asset of a company- are protected and are kept under the control of the partner
8. there is no central point of failure for the business process.

Phase	Security	Contract	Business Process	Business Benefits
Discovery	TrustCoM uses standards based security federation profiles such as SAML that makes integration easier and does not in principle hinder collaborations.	TrustCoM Reputation service can indicate past performance and the reliability of a partner.	A standards-based business process description language- CDL- can be used that enables partners to implement their required roles and match their internal activities to suit.	• Reduction of risk through reputation measures of business competency • Precisely defined business activities can be defined, reducing operational risks • Standards based security improves interoperability and reduces integration costs
Formation	Security is federated with identity management no longer centralised. This removes the need to register partners directly.	An electronic agreement with links to the technical policies- SLA and security- is presented and can be inspected before agreeing to participate. Contract can be accessed online and if necessary modified.	A service is deployed that represents the partner's role in the collaboration. This can be done very quickly.	• Security administration costs are reduced • Business process roles are quickly activated and configured- time to market is reduced.
Operation	Run-time policy-based security that is under the control of each partner. If necessary, a partner can disable access to services if a threat is detected.	Automated monitoring of service performance and comparison with an electronic contract. Overall business performance can also be monitored and recorded in the Reputation service. Exceptional events can be generated and processed by pre-defined policies which automate administration.	Web services are automatically invoked by systems to co-ordinate activities. Exceptions can be dealt with by the TrustCoM Policy Service. Poorly performing partners can be replaced by the VO Management system without reconfiguration of the business process	• Automated administration of services reduces costs • Automated membership management
Dissolution	The security federations can be disabled at a relatively few number of points by the VO Management system. Access to services is then disabled.	SLA is retracted from the SLA evaluator when the partnership ends.	Clean termination of processes and activities is possible as	• Security restrictions can be brought back into place at the end of the collaboration.

Table 5 Improvements from using TrustCoM RI in the CE Demonstrator

4.4 Improvements in other Product Lifecycle Phases

The TrustCoM VO Lifecycle model could in principle be mapped directly onto the Product Lifecycle model itself. In this section, we briefly consider two other phase of the product lifecycle which may allow other applications of the TrustCoM Framework.

4.4.1 Manufacturing

The main benefits arise from automation of supply chain management and the ability to dynamically change members within the supply chain as a 'virtual organisation'. The notions of partner 'service' and 'performance' would need to be modified in this particular scenario, but the principles are the same as demonstrated in the collaborative design phase of the TrustCoM CE Scenario.

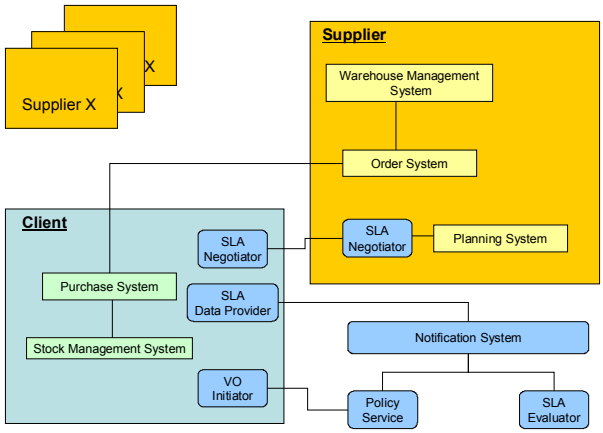

Figure 12 TrustCoM SLA management applied to the Supply Chain Management Problem

The service providers are now providers of actual hardware commodities and the VO is now composed of manufacturing facilities, component suppliers, logistics etc etc.

The collaborative business process would take form shown in Figure 13. Note that it is intended to give a general impression of the actors involved, the possible internal activities and the top-level interactions between the partners. It also includes another actor- a Logistics company- that would deliver the goods to the purchasing company premises.

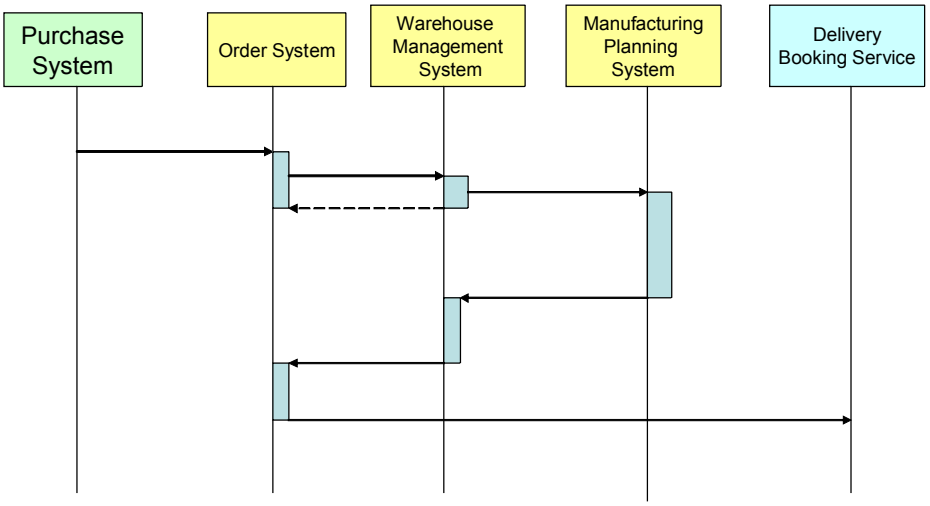

Figure 13 A VO of systems integrated across a supply chain

With automation of supply chains as Virtual Organisations, two things become possible:

- Reduction of personnel costs through automation of supplier management
- Just-in-time purchasing that makes the component purchasing process more flexible and ultimately reduces costs of component orders and their storage.

Performance of suppliers would be based on delivery time and quality of components delivered, so the appropriate SLA monitor would have to be developed that would be relevant for this model. It would also require integration with human-oriented workflow systems as well.

Policy-based administration would enable exceptional events to be detected and managed by the system. By being policy-based, human intervention is eliminated (or at least minimised) and administrative costs are reduced.

TrustCoM also supports the concept of dynamic membership as a fundamental aspect of the system. This could further automate the management of suppliers by using SLA as a measure of supplier performance. The author guesses that this step would require a great number of internal trials and experiments to understand how far this VO concept can be pushed to supplier management.

4.4.2 Product Support

Information on products needs to be available across the value-adding chain, particularly in the product retail and product support phase. This requires information systems from different business partners to be integrated together and conceived as a collaborative business processes. Access controls to these services becomes very important as the information is sensitive and should only be released on a need-to-know basis.

Various value-adding partners could be added or removed from the value-adding chain during the support phase- eg, a role that involves servicing and maintaining a customer's assets could be outsourced on a temporary contract basis.

The following diagram shows a possible collaboration involving a customer (pale green), a product support company (light yellow) and the original manufacturer (pale blue). A report is made to the Customer's Asset Management that describes a fault in a particular asset belonging to the customer. This issues a request to the product support company and as part of the diagnosis activity a request is made for information from the Engineering Product Data Management system hosted by the OEM.

The necessary information systems that participate in this scenario would be loosely integrated using the TrustCoM Messaging infrastructure and the TrustCoM Security system would ensure that the messages would be protected in transit between the partners. Access control policies would be deployed to ensure that the product support company could only access particular sections of the product database and only within the context of this collaboration.

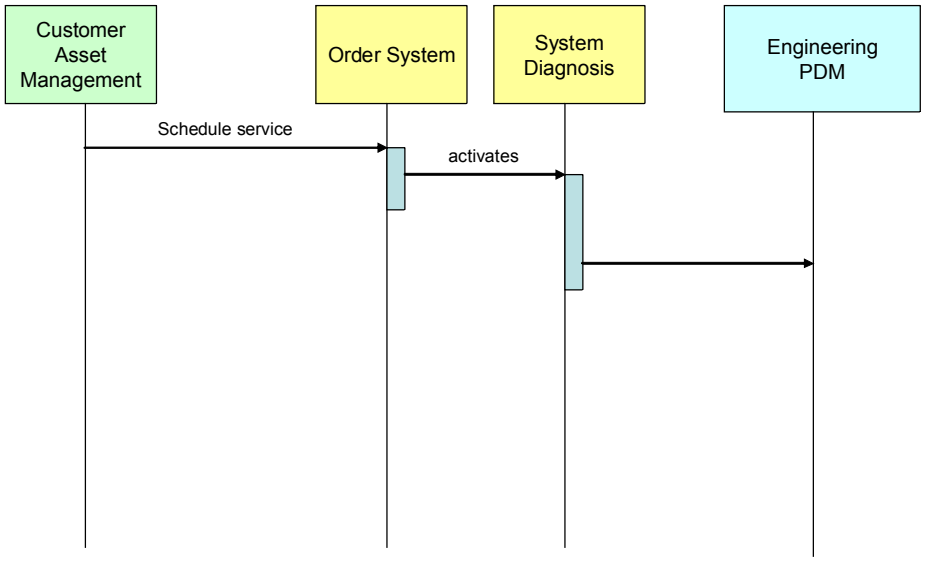

Figure 14 A VO for the Product Support Phase

5 Future Work

The demonstrator integrates a number of important TrustCoM components with non-trivial application services and demonstrates some new capabilities for an SOA based system. However, further work is required for making this business prototype more robust and attractive for future use.

At this current time, the most likely development of the Demonstrator will be within pilot studies conducted by BAE SYSTEMS on its internal network and to limited collaborations on the Open Internet through the UK CFMS project, for example. In the longer term, as confidence with this technology grows, then wider scale collaborations become possible. This 'incubator' would be used for presentations to internal product teams to foster interest in the TrustCoM framework and its future development.

This section enumerates the requirements for both the near-term and long-term objectives. Some of these are related to requirements detailed in the evaluation report.

5.1 Near Term Objectives

5.1.1 Infoset Generation

This is now identified as a critical aspect of the framework and one that hitherto has received the least attention due to the research priorities required for the project.

A critical future requirement identified in the evaluation report is the ability to easily compose the infosets required for the different TrustCoM sub-systems.

Security	Contract	Business Process	Policy	Service/Infr
• XACML policy editing tools	• SLA template editors and repositories • GVOA template editors and repositories	• Improved tools for generating CDL from UML or equivalent visual editor systems	• ECA Policy editing tools	• Event types need to be defined

Business Perspective

The ability to compose these complex documents becomes a limiting factor to the take-up of TrustCoM. Generating the correctly formed, precisely defined infosets for TrustCoM can be slow and prone to errors. This can critically reduce the formation phase whereby agreements and policies need to be generated for the new collaboration. If the skills required for composing these very technical documents is too high then this may prohibit service providers or even customers from participating in TrustCoM type collaborations.

5.1.2 Discovery Phase

Internal discussions within the company indicate that discovery of the correct service that meets functional requirements is an important issue. If an online economy of services is to expand then meaningful annotations need to be applied to the services so that they can be quickly discovered.

The SLA negotiator also needs to be integrated with the internal resource management systems that monitor its current load and its projected future load.

Security	Contract/Performance	Business Process	Service/Infrastructural
• Ensuring that partners meet top-level security requirements.	• SLA negotiator needs to be integrated with internal resource management systems to ensure accurate estimates of SLA performance are possible. • Reputation metrics need to be understood for effective discovery of new partners	• Order and purchasing systems need to be integrated so that processes for quotations and estimates can be automated.	• Meta-data annotations of services for efficient discovery

Business Perspective

The ability to effectively describe a service-capability is essential to both suppliers and consumers of the service. Service providers can only maximise their revenues if their products are easily discovered by their target end-users.

The ability to precisely identify the required services for collaboration is also necessary in order to reduce risk. A collaborator service must have the required capabilities to correctly enact a business role and this also needs to be satisfied at the earliest possible stage of the collaboration.

5.1.3 Formation Phase

In the present version of the system, the relevant security XACML policies are received by each partner from the VO Initiator, inspected and then injected directly into the PDP hosted by each partner. In the next phase of development, this should be replaced by a new mechanism that ensures that security requirements are respected externally and internal security requirements are respected as well. The motivation for this comes from the CE requirement for data security discussed in the Evaluation Report. Therefore, the initial XACML policy should be regarded as a security *requirement* document that needs to be modified by the service provider before it becomes an acceptable policy that can be deployed. The VO Initiator would need to be provided with an assurance- possibly a copy of the modified policy- that the external security requirement continued to be respected in the modified policy after this internal editing phase.

In the current implementation, the PEP is assumed to be hosted on a trusted network. In the case of un-trusted networks where rogue internal operatives (or even spyware) may be present, then messages to the PEP must be signed to ensure that eg, replay attacks are prevented.

Finally, the GVOA is not, as the author understands it, digitally signed by all of the partners as they enter the VO. This needs to be supported if the formation of the VO is to be legally completed online.

Security	Contract/Performance	Business Process	Service/Infrastructural
• A security protocol for defining security requirements rather than injection of policies	• Reputation metrics need to be semantically expressed • GVOA needs to be digitally signed by all partners	• Conversion of CDL to internal representations other than BPEL	• PEP component needs to ensure that internal messages to it are protected • All messages must be protected between the TTPs and the VO

Business Perspective

A business should always maintain control over its own security policy. At the current time the scenario assumes that the security policies are the correct ones that need to be deployed by each member without modification or enhancement. This needs to be extended so that security requirements are now stressed and that each member deploys a policy that suits not only the consortium but also observes internal security requirements as well.

The message traffic between the supporting systems in the VO could disclose sensitive commercial information. These messages need to be protected to the same level as the business application messages between the partners.

5.1.4 Operational Phase

In the current scenario, there is a use case that involves a provider re-configuring its internal system to re-direct messages to alternative internal resources. This ensures it can meet an external commitment by re-assigning its resources. However, if this were done in an extended enterprise where systems are distributed over different political zones, and one of these was in a country that was subject to export restrictions then this would cause obvious legal difficulties. In this case, the requirement would be for the client's data to be annotated with these security requirements- 'classification markings'- that can be interpreted and enforced in the infrastructure of the company. This assumes that the other parties run this infrastructure in good faith and do not attempt to cheat the legal agreement.

Another measure is to introduce transaction support in running business processes. This is a standard precautionary measure to ensure that in the event of a business activity failing then the relevant systems can be reverted back to their prior state.

Another area for improvement concerns supporting long-running activities and transactions. In the case of the CE Demonstrator, the Decifer Web site client interacts with the Decifer Partner service to activate a job, which in certain cases may take hours-days to complete. The practical solution that was adopted was to activate a Thread on the service that would enable control to be immediately returned to the client. In the general case, a better solution would be to ensure that the incoming message would be directed to an internal enterprise messaging bus

where request messages are queued, processed and responses returned at some point in the future. This would cleanly separate the web service from the business logic executed within internal business systems.

It would also be desirable to integrate the engineer end-user into the VO in the following sense. In the present version of the Demonstrator, the engineer has her/his own security relationship with the web site that enacts the DeciferClient role. The DeciferClient then interacts with the relevant member services on the client's behalf. Assuming that the web site could be used by a large number of people, it would be better to adopt a federated security model so that identification is performed locally. This could, in turn, be integrated with the TrustCoM Federated security system. This would enable clients to sign in once and access a federated set of web sites using the same security profiles and configuration as for the VO web services. This would reduce administration and increase flexibility within the VO.

Finally, the business process must recognise the importance of human actors within critical business-decision activities. The business process must integrate not only internal business systems (as represented by web services), but also workflow systems as well.

Security	Contract	Business Process	Service/Infrastructural
• PDP system needs to be supplemented with attributes extractor • Meta-data annotations to messages to ensure that security requirements are observed at run-time • All messages between the VO and TTP need to be encrypted and signed • Web browser client security should be integrated with VO security model.	• The agreement should specify the security requirements of data as it is being processed in other domains administered by other partners.	• Integration with workflow systems for supporting human actors should be made • Transaction support must be provided	• Enforcement of meta-data requirements on client data. • PEP must have the ability to deal with high volume message transactions • TrustCoM messaging system must be integrated within internal enterprise messaging systems, such as message queues

Business Perspective

Not all business decisions can be automated and so collaborative business processes as conceived by TrustCoM must be integrated with workflow type systems in some way. This reduces risks by enabling key business specialists to make the correct decisions at the correct time.

The security of the data once it enters another partner's domain causes the greatest concern to a partner. Providing assurances that the correct security measures are

being followed in that partner's enterprise would help to strengthen the business relationship and prevent any intrusive, draconian measures being applied.

5.1.5 Dissolution Phase

All of the information generated in the VO- policies, SLAs, the CBP, GVOA itself- need to be stored in a secure repository for possible future reference. At the present time all of the data is stored in different locations that could make retrieval difficult. At the very least, there should be the ability to retrieve all of the historical data that was generated during the lifetime of the VO with a clear statement on its provenance.

Business Perspective

At the point of dissolution of the partnership all historical data, including in certain cases all of the transactions made, needs to be stored. This would provide assurances that if difficulties and complications occur- eg, the overall business goal is disputed with the customer- then all relevant technical information is stored for future audit purposes.

5.2 Long Term Objectives

Long term objectives concern those areas that could not be fully addressed in TrustCoM and which require further research.

Looking at the current practice for putting together a VO in TrustCoM, it is clear that there is some reliance on human actors for putting it together using the web browser based VO toolkit. In more futuristic scenarios, one could envisage a VO Initiator designing his/her business process and then requesting the VO management system to go out and discover AND enrol members automatically through an agent-based negotiation system. This of course touches on many controversial points on how much control should be delegated to machine systems. This is particularly the case for CE where the services and processes may be complex, have different interfaces and where performance criteria may be difficult to define.

However, whatever progress can be made towards this vision, it is certain that if the market expands one has to have technologies that can make the entry time shorter, and make the dynamic business environment safer, stable and operate with minimal risks.

One could say that some of the critical areas are:

a. **Semantic web support**- In the CE Scenario, there may be many types of optimisation service and evaluator service, with different variations on the interfaces and behaviours. Therefore one has the problem of locating the required service for the need of the VO. To improve the 'discoverability' of services, each should have a description bound to it that characterises its technical capabilities. This potentially reduces the

time spent searching for partners required for fulfilling the required technical roles. It also improves the chances of service providers making more revenue.

b. **Policy refinement**: though the TrustCoM framework has begun to make stronger associations between the business/legal and technical aspects of an SOA, there are formidable challenges associated with policies and other technical documents that have connections with business and legal requirements in general. It would be desirable to have a framework that would enable high-level organisational/business policies and objectives to be translated into machine-understandable artefacts such as the CDL, XACML, ECA and SLA documents used in the TrustCoM RI. This would reduce errors and hopefully make time-to-market quicker as well.

c. **Formal modelling of business processes**. The challenge is now to automate as much as possible other aspects such as the management, inter-partner negotiation activities. These are potentially complex processes that involve high risk to a company if they are mis-managed. Formally defining them while ensuring that business flexibility is maintained would be a first step towards improving the performance of discovery and formation of the VO.

6 Conclusions

This study has attempted to use the most mature and stable parts of the TrustCoM RI within a business prototype. In contrast with the CE Test Bed more realistic applications are used that highlight some of the integration challenges from using other web application solutions within the TrustCoM framework. Resolving these has been important experience in understanding how TrustCoM could be used in association with in-house application services for CE.

Technical achievements:

- The basic critical requirement for security has been met. Members can be quickly enrolled into a security system that protects business messages and controls access to the services they contribute to the VO.
- A critical requirement for service monitoring has been demonstrated. This enables basic commodity services for HPC and storage to be plugged in and monitored using technical metrics that can be easily shared and compared with electronic agreements.
- The VO toolkit provides valuable support in setting up and operating a VO. The discovery service enables new commodity service providers (HPC and storage) to be identified on the basis of their reputation and agreed performance and presented to the VO Initiator.
- A limited VO Membership management function has been demonstrated. This enables HPC and storage members who default on their SLA to be managed and limited corrective actions to be taken without human intervention.
- A demonstration of internal resource management has been made, indicating how a service provider can take corrective actions in the event of changes in the available capacity of an internal resource
- A demonstration of how SLA monitoring can be linked with penalty mechanisms. This demonstrates how SLA can be used as an incentive for a supplier to maintain an agreed performance target.
- A set of realistic applications- GRIA and Decifer- have been deployed and successfully integrated within the TrustCoM framework. This experience has revealed a strategy for integrating other application services into the TrustCoM framework.

The business benefits from using TrustCoM are determined to be:

- Reduction of risk by protecting critical assets such as design data and other intellectual property within the collaboration
- Risk reduction through continuous monitoring of partner performance.

- Reduced administration costs through continuous comparisons of required partner performance with electronic agreements.
- Reduced time-to-entry for the collaboration- the federated security system in TrustCoM precludes explicit registration of operatives between organisations who intend to share their web services.
- Reduced service administration overheads through a degree of automation- dealing with exceptional events through policy-based systems.
- Reduced security administration costs through use of federated security models
- Reduction of risk through sharing experience of partner/supplier performance through use of Reputation- an instrument for discovering partners
- Improved business flexibility through the ability to replace partners

Against these achievements, improvements are required in a number of areas before the framework can be taken up as a more advanced business prototype. In the near-term these include (in order of importance):

1. Tools for helping specialists with limited technical knowledge to create and modify the critical infosets that are required for the TrustCoM sub-system- such as the CDL, XACML, ECA policies and SLAs
2. Further integration of SLA negotiator agents with internal resource management systems- this would enable more accurate estimates of the internal capacity that can be committed to the VO that is being negotiated.
3. Support for GVOA negotiation, enabling legal terms and conditions and other elements to be negotiated online and eventually digitally signed by all parties.
4. A security negotiation protocol that enables potential members to make adjustments to required security policies for the sake of their internal security requirements
5. An enhancement to the messaging infrastructure to ensure improved message security on internal un-trusted networks
6. A mechanism for assured storage and retrieval of VO operational data- the event and business transaction data generated during the lifetime of the VO- that can

The most critical requirement is 1, where business specialists would require high-level business applications that would help them to compose business processes, agreements and policies that regulate the VO. Even with an extensive catalogue of templates, these kind of documents would require substantial modification to make them suitable for a particular business partnership.

The framework could be applied to other areas of the product lifecycle as well, including manufacturing and product through life-support. Preliminary ideas have been sketched to show how components from TrustCoM RI could be applied to the systems that would be involved with purchasing and product order systems.

7 References

1. TrustCoM Framework IV, TrustCoM deliverable D63
2. SIMDAT Project home page. http://www.scai.fraunhofer.de/710.0.html
3. GRIA Home Page http://www.gria.org/
4. CE Test Bed, TrustCoM deliverable D65.
5. Final Evaluation of the CE and AS Test Beds, TrustCoM deliverables D68+D68

8 Appendices

8.1 Appendix 1: Preparation Phase Information

This appendix section contains the technical data related to the 'preparation phase'. The preparation phase consists of the configuration and generation of all of the data that is required by the TrustCoM framework.

This concerns:

- STS configuration- business cards, STS keys- both public and private
- XACML access control policies
- Choreography definitions
- Event-condition-action policies
- SLA templates

8.1.1 STS Configuration

The STS has the following associated security information that needs to be generated:

1. The business card containing an organisation wide public certificate
2. The STS external certificate- required for identifying the STS to public clients and business partners
3. The STS internal certificate- required for identifying the STS to internal clients that wish to request security assertions or for checking the validity of security assertions

Business Entity	Role
Avio Systems (UK)	VO Initiator; no business process role
Aerosystems Inc (UK)	Decifer Client
Sci Eng Solutions Limited (UK)	Decifer Partner
EasyHPC (DE)	HPC Partner
iStorage (DE)	Storage Partner

Table 6 Business Entities and their Roles

All of the businesses above, with the exception of Avio Systems, require the three security documents for their STS configuration.

The following table describes the certificates and their common names used for this scenario.

Business Entity	Internal STS	Public STS	Business Card
Avio Systems	Avio Systems Internal STS	Avio Systems Public STS	Avio Systems
Aerosystems Inc	Aerosystems Internal STS	Aerosystems Public STS	Aerosystems Inc
Sci Eng Solutions Limited	Sci Eng Solutions Internal STS	Sci Eng Solutions Public STS	Sci Eng Solutions
EasyHPC	EasyHPC Internal STS	EasyHPC Public STS	EasyHPC
iStorage Solutions	iStorage Solutions Internal STS	iStorage Solutions Public STS	iStorage Solutions

Table 7 Common names for the three certificate categories by business partner

8.1.2 XACML Control Policies

The following table defines the XACML control policies that are required to be generated:

Partner	Permitted Role	Permitted SOAP Action
Decifer Client	Decifer Partner	• retrieveOptimisationWorkFile • notifyJobChangeStatus • registerJob
Decifer Partner	Decifer Client	• activateJob
HPC Partner	Decifer Partner	• run
Storage Partner	HPC Partner	• putFile • append

Table 8 Table of Access Control Policies used in the CE Demonstrator

8.2 Appendix 2: CE Demonstrator Architecture and Deployment Details

This section primarily focuses on the detailed aspect of the CE Demonstrator architecture using the TrustCoM components and services. Where it is appropriate to do so, some information on the deployment is also provided to clarify the description of the architecture.

8.2.1 Top-level View

The purpose of this view is to show the components deployed and their relationships and dependencies. The arrows on the connecting lines denote the dependency of one component on another. The reader should not deduce any protocols or sequences of interactions from this diagram.

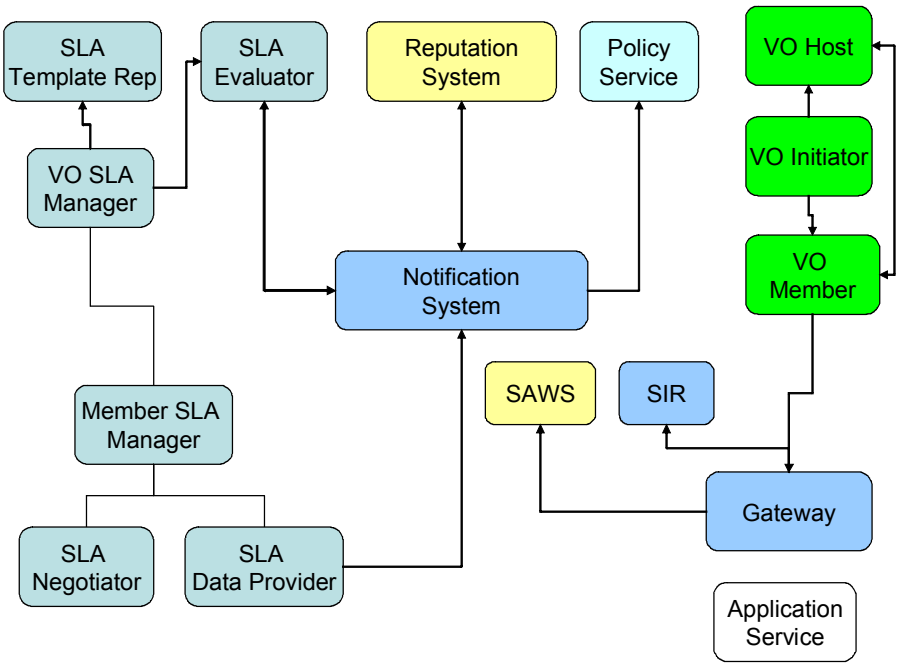

Figure 15 Top-level view of the CE Demonstrator Architecture

The first point to make is that the components group together other components and services. Also note that the application service has no dependency or knowledge of the other components, which is an aim of any SOA. It should also be noted the importance of the Notification System in communicating events and messages between the components. Certain of the components are both consumers and producers of events; components that are wholly consumers have no direct dependency on the Notification System. The Gateway contains many components and for simplicity these are aggregated into a single sub-system. One of these- the

8.4 Appendix 4: Installation and Configuration of the Gateway

The author records the installation and configuration of these components at some length here not out of sentiment, but as a reminder of the trials and challenges of installing them and out of a wish that others may not suffer the same fate. The author extends his personal thanks to Matthias Assel (HLRS) for helping him to compile the steps described here.

As noted earlier, the 'Gateway sub-systems' in the context of this report is not only the Gateway component provided by BT but also the PEP-SIR, PEP, STS and PDP components provided by other partners.

Note that the following steps are necessary for installing and testing of the gateway outside the VO Toolkit. The VO Toolkit simplifies the service instantiation within a particular federation- in the steps described below the VO Toolkit is not used and so this is done manually.

1. Install the PEP-SIR Java ant project
    a. Edit the etc/cfg/transport.properties to set the listening and forwarding ports
2. Install the BT-PEP Java ant project
    a. Edit the etc/cfg/transport.properties to set the listening and forwarding ports
3. Install and configure the STS:
    a. Copy the sts web application folder into some location in the IIS web folder hierarchy
    b. Change the properties of the folder to make it executable in IIS
    c. Enter the STS Install Helper folder and run the STSConfiguration Application
    d. In the STSConfiguration tool, open the STS web folder
    e. Click detect
    f. Select certificates- the CNs for public certificate, internal certificate and the issuer URL
    g. Issuer URL should be correctly set using 'Detect'
4. Restart IIS
5. Install MySQL database, Tomcat and OpenSSL
6. Install the Gateway database into MySQL
7. Install the Gateway war into Tomcat
8. Install the management interface for the PEP- mwsng war file
9. Start then stop Tomcat and edit the file 'gateway.config.properties' in the WEB-INF\classes folder – set the PEP mgmt address (mwsng), STS address, PEP operational, STS management and the PDP addresses. Also add the location to the real instantiator certificate-use the BT supplied copy for initial testing and trial use
10. Restart Tomcat
11. Go to the Gateway main page, select the Gateway Profile Manager link
12. Define the name of the federation, the PEP mgmt, PEP and other component network addresses except for GVOA and SLA- these are similar to the entries defined in the Java properties file defined in 9
13. Click on the Add New Federation Profile

14. Copy the UUID that is generated to the file federation.manager.properties and set it to the fedManager.default.federationProfile.id etc
15. At this point the gateway is configured and ready for messages belonging to a particular federation.
16. Tomcat should be re-started.
17. The Gateway is now ready for your own federations to be set up, eg, manually using the BT GatewayClients app (Gateway\GUIClient)- an example Federation Manager Client

8.4.1 Generating and Installing the certificates for the STS.

Type of certificates and keys required:

1. Organisational certificates and keys associated with the business cards. Used for signing assertions when exchanged between organisations…?
2. 'Internal STS certificates'- used for protecting requests made by internal actors, eg, the PEP, for security claims *within* the organisation
3. 'Public STS certificates'- used for protecting claims made by STS when the are transmitted between organisations
4. Instantiator certificates- used by the component used for instantiating a service within the organisation.

The STS requires 2 certificates and a business card:

1. STS Internal pfx must be stored in Local Machine/my (Personal certs)
2. STS Internal cer must be stored in Current User/my (Personal certs)
3. STS Public pfx must be stored in Current User/my
4. CA cert must be stored in Current User root and Local Machine root
5. Business card certificate for the business partner must be stored in Local Machine/my certificates folder- read access must be granted using EMIC's certificate tool. This ensures NETWORK_SERVICE is granted permission in Server 2003. Note that ASPNET in case of Windows XP must also be granted permission.

Notes

1. STS- install the certificates **before** using the STS Management tool
2. All internal STS and public STS certificates need to be generated for all partners

The keys and certificates used by the STS, PEP need to be correctly generated in order to ensure that different platforms and systems based on Java and .NET can work well together. In this particular case, a Microsoft 2003 Server CA was used for generating the certificates.

1. When using a Microsoft CA, generate client-side keys and certs only. Don't generate server-side certificates.
2. Ensure the private keys are exportable

3. Export the certificates in base 64 encoded format to ensure they are compatible with Java-based applications- in this case the PEP.