An assured environment for collaborative engineering using web services

David Golby[a1], Michael Wilson[b], Lutz Schubert[c], Christian Geuer-Pollmann[d]

[a]*BAE SYSTEMS Advanced Technology Centre, Filton, UK,*
[b]*CCLRC,UK,*
[c]*HLRS, University of Stuttgart, Germany*
[e]*European Microsoft Innovation Centre, Aachen, Germany*

Abstract: This paper describes an application of the TrustCoM environment to support secure contract based collaboration between companies using managed web services. The application scenario describes a consortium of engineering companies that seek to upgrade a customer's fleet of aircraft to provide in-flight internet capabilities. The environment supports the consortium to collaborate so as to take advantage of the market opportunity. In order to reduce the risks of collaboration, the environment provides assurances of the past performance of consortium members, of the current performance of each member to meet their contract and service level agreements, and the secure control of access to resources. As a result of a member's performance, the consortium dynamically reconfigures itself and initiates a collaborative business process that enlists new members to join and contribute to the negotiations with the customer.

Keywords: Virtual Organisations, TrustCoM Project, Collaborative Business Process, Federated Security, Service Level Agreements, Service Oriented Architecture

1. Introduction

Collaborations within the engineering sector are a means of reducing risk in the development and support of highly complex or novel products over the product lifecycle. The collaborators often include tier-1 suppliers, system integrators, component suppliers, engineering consultancies, maintenance companies, and product disposal companies. The size and scope of collaborations may vary considerably over the product lifecycle. In a consortium, each partner can focus on its core competencies but must align the complex collaboration processes with the rest of the collaboration. The virtual organisation (VO) model is therefore a good fit to these many different collaborations, whether they are legally bound as a joint venture, or through a set of contracts and co-ordinated behaviours between a customer and its chain of suppliers.

The aim of the TrustCoM project is to devise a software environment built upon a sound conceptual framework for such VOs which will provide an infrastructure to

[1] Corresponding Author: David Golby, Advanced Technology Centre, BAE Systems PLC, PO Box 5, Filton, Bristol, BS34 7QW, UK; E-mail: david.golby@baesystems.com

support companies' flexible response to market opportunities, reduce lead times to market by maximising the benefits of the concurrent engineering approach, while minimising entry cost to collaborations and ensuring that all interaction within the collaboration is secure. The project will deliver a conceptual model, system architecture with software profiles [1], and a reference implementation which will be evaluated through a set of industrial demonstrators [2]. The industrial demonstrators include scenarios on eLearning and collaborative engineering (CE) - the subject of this paper. The TrustCoM framework and software environment must address issues from many disciplines including legal, socio-economic, security, contract and service level agreements, business process and industrial application domains.

This paper presents the CE scenario and assesses the benefits of TrustCoM technologies to CE in general. We focus on the design phase of the product lifecycle, though the general ideas are applicable to other phases as well.

2. Assured Environment Issues

Within an engineering collaboration, the business risks reduced by collaboration should not be replaced by other risks inherent in the collaboration itself. To maintain collaboration, it is necessary to transfer data between collaborators, and to inspect services and resources which are embedded within each others local IT infrastructure. The decision makers who use this information may range from high level policy makers to engineers who need additional information from their partners if they are to execute their tasks correctly. For example, the management of production processes can be aided if information on the status of a supplier and the progress of an order through the multi-tier supply chain can be correctly monitored. A designer may require critical interface and behaviour information on a partner's subsystem in order to optimize the design of the particular subsystem that he is responsible for. Finally, product and asset information will be needed throughout the operational and decommissioning phases for training, maintenance and product disposal.

TrustCoM reduces the risks inherent in collaboration by addressing the complete collaboration life cycle, and providing assurances at each stage of its operation. The selection of partners is based on assurances of their previous performance in a role – their reputation or supplier qualification. A collaborative business process model (BPM) provides transparency to all collaborators of each others' roles. Service level agreements (SLA) provide assurances of the performance on time, to quality and cost of each collaborator in their role. A contract provides the assurance of contingencies should a collaborator fail to fulfil their role. Claims-based access control is used to provide assurances of the identity of each party, and the authorisation for access to the services and resources that they need to undertake their role – and only access to those services and resources and no others.

3. Architecture and Standards Conformance

The TrustCoM architecture is designed to provide the required assurances, monitor conformance to contract, SLA and BPM, and enforce access controls whilst also minimising the initial costs of adopting it, and maintaining flexibility for each collaborator who may be involved in many other activities at the same time.

A service oriented architecture (SOA) has been adopted to provide flexibility over the geographical distribution of the collaborators. The location transparency of SOA allows collaborators to move the physical location of services as they wish without disturbing the operation of the collaboration. The main risks of exposing a company's services through an open SOA are mitigated through the security assurances provided by the TrustCoM architecture.

The environment has been designed using existing open web service specifications rather than develop the environment entirely as a proprietary system. Although this adds considerable cost and complexity to the design, it also increases the transparency of any implementation, and eases third party implementations of the framework. Both these factors should increase both the trustworthiness of the environment and the probability of its adoption. A number of possible representations of the framework are possible, but the following diagram shows the sub-system view where the responsibilities of the individual sub-systems are shown along with their interactions with each other in the context of an executing collaborative business process within the VO. Note that all of the components are embedded within an 'Infrastructural' component that provides many value-adding services of its own in the lifecycle of an application service.

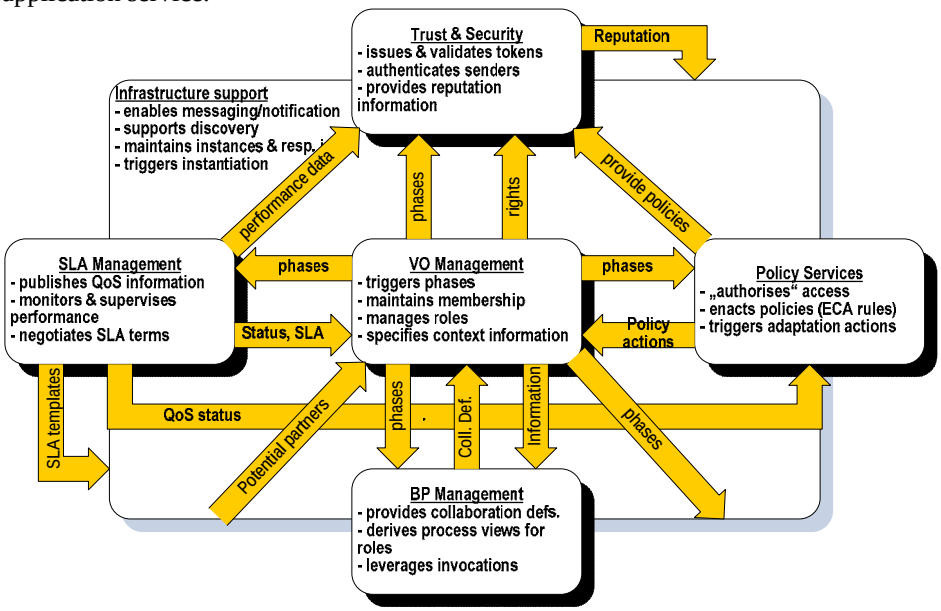

Figure 1. the subsystem segmentation of TrustCoM

In order to minimise integration costs, potential collaborators must satisfy minimal requirements: the application services must be exposed as web services, provide a WSDL interface definition, and maintain a WS-RF resource so that the web service can be managed. This approach maximises the opportunities for providers to re-use services in other collaborations, even outside the TrustCoM assured environment.

The core part of the TrustCoM environment could be operated by a third party whose role is to host the environment for a fee, or by a member of the collaboration. The business models that drive this choice suggest that for small and short lived collaborations, a third party is more likely to provide the environment, while for large

and long term collaborations, such as the collaborative engineering scenario considered here, the second option is more likely to be adopted.

The main role of the environment is to map from a contract in natural language that can be legally binding, down to executable policies, BPMs for each organisation, SLAs for each service and access controls across the distributed services needed to operate the collaboration.

The architecture provides a VO management subsystem to host the natural language contract and hand drafted XML policies matching some clauses, and a database of the VO membership and the access details of their services which are together termed the General VO Agreement (GVOA). The business process of the collaboration is defined by hand in UML, which is refined into WS-CDL and supports conversion into an executable BPEL description for each collaborator that calls their own services and those of other collaborators that they interact with. For each service, the SLA management subsystem stores an SLA. The SLA mgmt subsystem monitors performance of the service and raises events when any aspects of the SLA are breached. The executable versions of policies in the contract are loaded into the policy subsystem where they are executed when events from the security, SLA or BPM subsystems raise events that trigger them. The security subsystem includes security token services (STS), policy enforcement points (PEP) and policy decision points (PDP). PEPs enforce access control policies loaded from the GVOA, accepting security tokens from known STSs such as those operated by collaboration partners. The security subsystem also includes a reputation service that stores a record of the performance of each collaborator (for potential usage across different VOs), and issues reputation status events which can be used to trigger policies derived from the contract if the reputation falls below a threshold. The whole architecture is hosted on an infrastructure which transmits the events between the subsystems as a subscription based notification service.

In the design and implementation of the TrustCoM hosting environment, the following open specifications and standards have been adopted: SOAP, WSDL, WS-Addressing, WS-RF, WS-Notification, WS-Trust, SAML, XACML, WSLA, WS-Agreement, WS-CDL and BPEL. We have created multiple profiles that define how we use combine different specifications: we selected a subset of WSLA to support a collaboration environment; we specify a combination of WS-Trust and SAML to support a VO-centric claims-based security model; we define how XACML should be used for web services and transport formats for policies in XACML; and we define how WS-CDL can be used to represent collaborative business processes between organisations that can be refined into executable BPEL for each organisation.

The overall architecture, design and implementation of the assured environment is designed to meet the needs of a wider variety of business models and collaboration patterns than used in the collaborative engineering application described in this paper, but its operation is being demonstrated, and will be evaluated, in that domain.

4. The Collaborative Engineering Scenario

TrustCoM has developed several industrial scenarios in order to test, validate and refine the TrustCoM framework through the derivation of requirements, testing of the feasibility of ideas and application of use cases for the verification and validation of the reference software implementation of the TrustCoM framework.

The storyboard for the CE Demonstrator considers a pre-contract scenario where a business proposition is made by an engineering consortium to a customer to upgrade its products. The principal actor in the scenario is an existing engineering VO (called 'CE VO') that is responsible for the design and manufacture of a high performance business jet. The CE VO works with a number of different entities, including engineering consultancies, tier-1 subsystem providers (in this case, of the in-flight internet capability) to generate a number of proposals to the customer. The business proposal is to upgrade the customer's fleet to provide in-flight internet and other services in the passenger cabin. The goal of the collaboration is to win a contract that satisfies the customer's requirements, minimises risks involved with delivering the aircraft upgrade and maximises the benefits to the consortium members. During the negotiation process, various parties access information and computing resources hosted by different collaborators to make decisions. For example, the designers have access to asset information systems held by the customer's maintenance provider, while the designs are accessed by an external engineering consultancy. The engineering consultancy itself uses services from other companies, two of which provide High Performance Computing and storage (HPC) services.

Figure 2 presents the top-level view of the actors within the collaboration. From the figure, the collaboration can be recursively broken down into 'sub-collaborations' where for example, the 'Analysis VO' aggregates services from engineering consultancies, software houses and HPC providers to provide an overall capability that could be applied to different engineering sectors. This overall capability provided by the Analysis VO would participate within the overall design cycle to assess designs and possibly help to improve them as well.

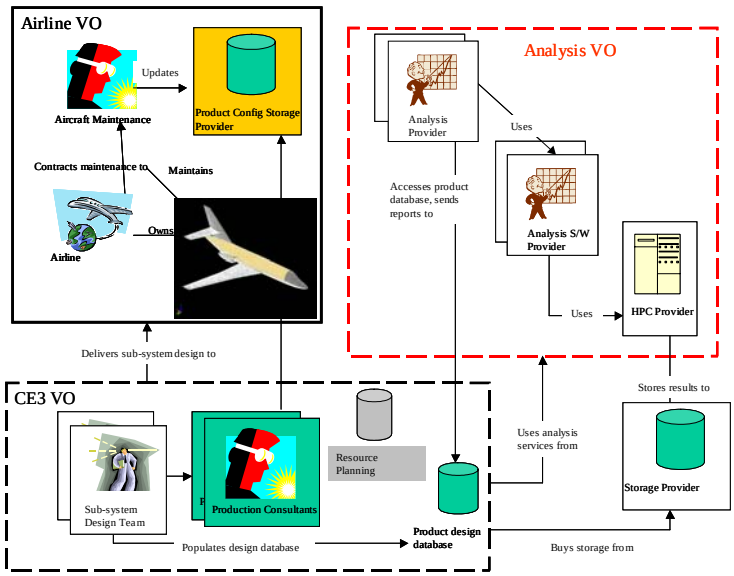

Figure 2. The actors within the CE Scenario

The collaborative business process is a fundamental aspect of the TrustCoM VO model, and this can be expressed as a simplified UML activity diagram shown below in Figure 4. Other collaborative business processes derived from this picture can also be

identified at the lower levels of the collaboration as well, e.g., between the HPC and SP services shown in Figure 5.

Currently, the TrustCoM CE Test bed is used to examine particular aspects of the scenario described above in the assessment of the TrustCoM technologies. The CE Scenario is considering the following aspects within more detailed studies:

1. Secure business process enactment
2. VO Management and Evolution
3. Infrastructural Aspects

In the *secure business process enactment* study, we use a federated security model to enable collaborators sharing their services. We use SAML tokens with embedded claims to protect outgoing messages. Such a token could e.g. contain that *"requestor from partner A of this service has the role 'Analyst'"*, which can be used by domain B to make an access decision. After validating the claims, the service's policy enforcement sends an XACML request to a policy decision point that is used for making the final access control decision. The policy enforcement also ensures that the actual messages are protected appropriately, e.g. signed and encrypted message contents. This separation simplifies application development, because security requirements are enforced by specialised components. Figure 3 shows a simplified picture of these components in the context of the HPC and Storage Provider services.

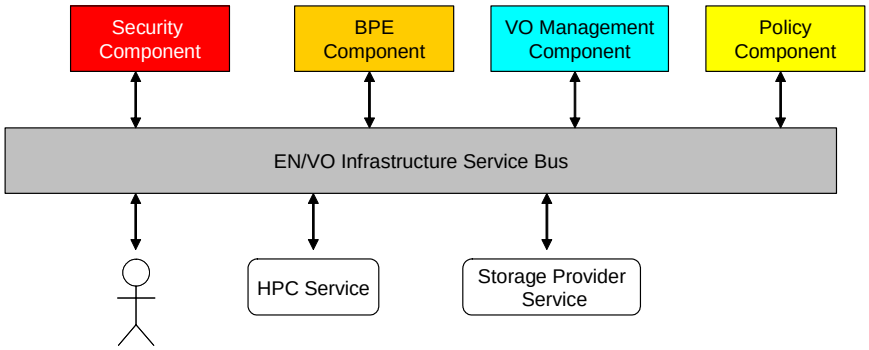

Figure 3. EN/VO infrastructure service bus connecting application services and TrustCoM components

So for example, the outgoing message from the client/Analyst on the far left of the diagram will be intercepted by the service bus (the Infrastructural sub-system in Figure 1) and the aforementioned security claim inserted into the message by the Security sub-system. This claim can be validated at the HPC Service provider's site using its own Security sub-system before the message reaches the application service itself. In this way, the clients and service providers can collaborate without having to participate within any intrusive security procedures. Securing the message rather than using a private link also gives much greater flexibility and admits the possibility of, for example, the routing of messages through many domains and over different transport protocols while ensuring end-to-end security of the message.

Secure business process enactment will further consider how the top-level business choreography expressed in Figure 4 as WS-CDL can be distributed as BPEL documents to each collaborator for them to enact. In Figure 3 above, the BPE sub-

system becomes the primary co-ordinator of this collaborative business process in that it ensures that the application services (eg, the HPC and Storage provider services) are executed in the correct sequence as required in the collaborative business process description that is part of the GVOA. As shown in Figure 1, the BP management component also reports any exceptions to the VO Management sub-system which may take measures (defined by the Policy sub-system) to manage these exceptional events.

This approach ensures that a distinction is made between the public interfaces and message interactions of each collaborator in the collaborative business process, and the private processes that are used for fulfilling the business duties of that collaborator. The EN/VO infrastructure will also provide support for the management of the context of these interactions via WS-Coordination. This is an important ingredient for other value-adding features, such as transaction management, as well.

In *VO Management and evolution*, the problem is addressed of how the VO reacts when individual members such as the HPC service provider violate the agreement binding them to the VO- the GVOA described earlier. For example, the agreed SLA of the HPC service provider within the GVOA could be violated and the performance of that service could fall below a certain threshold. Under these circumstances, a VO policy dictates that the service has to be monitored and messages to and from that service logged to an audit service. Furthermore, a reputation service (part of the Trust and Security sub-system in Figure 1) can be used to record a change in the reputation level of that service – important information that can be used by current or future users of that service as one of many criteria for selecting that service in the VO discovery phase. If the performance level declines further, the current HPC provider could be replaced by an alternative service provider who can take over the same roles and responsibilities. The ultimate aim of TrustCoM is to ensure that this process of discovery of alternative suppliers, their enrolment into the VO and their monitoring can be managed in a seamless, automated way.

Infrastructural aspects will consider how the EN/VO infrastructure can provide means for supporting the 'instantiation' of an application service and its configuration for a particular collaboration or VO. Application services can therefore be deployed once and 'instantiated' and configured for many different engineering collaborations.

The following diagram shows the top-level business collaboration that is enacted within the collaboration described in Figure 2. This is a view of the collaboration that is familiar to engineering project managers who ensure that the business and engineering teams are co-ordinating their activities correctly.

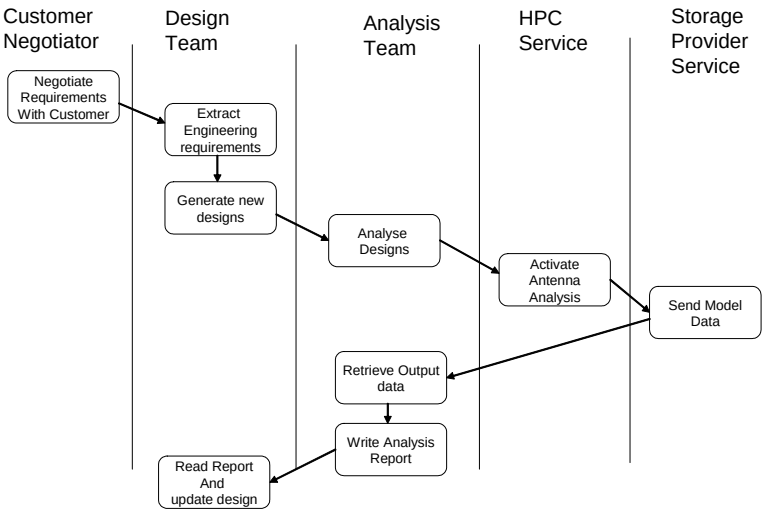

Figure 4. The Top-level collaborative business process in the CE Scenario

Figure 5 shows the collaborative business process fulfilled by the HPC and SP services. This operates at a 'lower-level' of the collaboration but is still required in order to ensure that the business interactions- such the order or expected interactions, the type of messages etc, are declared ahead of the process being enacted.

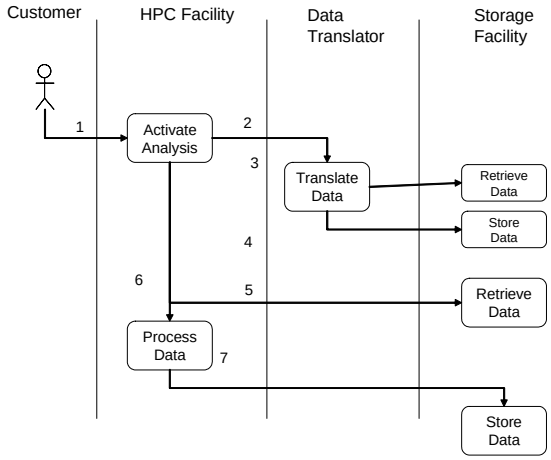

Figure 5. A collaborative business process involving the HPC, Data Translator and Storage services

The technologies described above will be assessed for their benefits in meeting business requirements (both functional and non-functional) and improving business performance. For example, all of the systems described here should be easy to administer and provide greater reach to the administrator, thereby automating repetitive tasks and eliminating redundancy. Business performance improvements are difficult to quantify and assess, but where possible we shall try to compare current procedures (such as those involved with the registration and management of individuals within a PKI based security system, monitoring of service performance, service configuration and administration and so on) with the simplified procedures associated arising from the use of TrustCoM technologies.

5. Conclusion

The CE scenario indicates that the TrustCoM environment could benefit engineering collaborations in different ways. First of all, it leads to an improvement in the modelling and design of the collaboration at the process and agreement level, leading to clearly defined business roles and responsibilities defined by agreements. This potentially enables a small group of top-level business policy makers to design a collaboration that can be fulfilled by the many potential service providers that are accessible via an Enterprise Network. This collaboration can then be enacted by these service providers who are discovered by the VO management subsystem and whose membership is regulated by an agreement defined by the VO designers. The ultimate goal is to introduce automation into the collaboration wherever possible, ensuring that IT systems can be connected together in adaptable ways (as in the case of the federated security) and combine different points of view on the collaboration, such as legal specialists, into the agreement that binds the VO together. From the viewpoint of the service provider, using TrustCoM enables his services to be used within many different types of collaboration with only minimal administration overheads.

The project is currently in the final development and testing phases and will commence an industrial demonstration phase next year. Therefore, the results should be regarded as in their preliminary state and indicative of how the technologies from TrustCoM could be applied to collaborative engineering in service based economies.

Acknowledgements

The work reported in this paper has been partially funded by the EC through a FW6 IST programme grant to the TrustCoM integrated project under contract 01945. The project partners, who have all contributed to the work reported in the paper, are: Atos Origin, BAE Systems, BT, IBM, Microsoft, SAP, CCLRC, ETH, HLRS, SICS, SINTEF, and the universities of Kent, London (Imperial and King's colleges), Milan and Oslo.

References

[1] M D Wilson, A Arenas, L Schubert, The TrustCoM Framework for trust, security and contract management of web services and the Grid - V2, *RAL Technical Reports*, RAL-TR-2006-003, (2006) http://epubs.cclrc.ac.uk/work-details?w=35146

[2] T Dimitrakos, D Golby, P Kearney, Towards a Trust and Contract Management Framework for Dynamic Virtual Organisations, *Proc. eChallenges 2004*, Vienna, Austria, 27-29 Oct (2004).