Deliverable

38

WP38

Migration and Demonstration Plan for Ad Hoc Aggregated Services Demonstrator

This is an updated version of D38 and includes a description of the initial version of the demonstrator (D57).

Paul Kearney, BT

15th February 2007

Version 2 Draft C

TrustCoM

A trust and Contract Management framework enabling secure collaborative business processing in on-demand created, self-managed, scalable, and highly dynamic Virtual Organisations

SIXTH FRAMEWORK PROGRAMME

PRIORITY IST-2002-2.3.1.9

Networked business and governments

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

Activity:

Work Package: **WP38**

Task:

Document title: Migration and Demonstration Plan for Ad Hoc Aggregated Services Demonstrator

Version: **Issue 2 Draft C**

Document reference: **Deliverable D38**

Official delivery date: **February 2007**

Actual publication date:

File name:

Type of document: Report

Nature: Public

Authors: Paul Kearney, BT (main author)

Reviewers: Lutz Schubert, HLRS

Dave Golby, BAE Systems

Approved by:

Version	Date	Description of version and changes
Skeleton draft	12/6/06	Outline of deliverable. Limited circulation. Discussed by phone conference 12/6/06.
Draft A	14/7/06	Largely complete draft circulated for comment within WP38 team.
Draft B	20/7/06	Changes to partner role allocation table following phone conference.
Draft C	25/7/06	Incorporation of comments from David Chadwick.
Draft D	7/8/06	Revision and incorporation of comments received to date.
Draft E	7/8/06	Cleaned up version of Draft D (changes accepted, comments removed)
Draft F	15/8/06	Update taking into account comments from SAP.
Issue 1.0	15/8/06	Cleaned up version of Draft F (changes accepted)
Version 2 Draft A	13/2/07	Draft in response to feedback from project reviewers. The main additions are in the new Section 4 onwards. Draft A is a mostly complete draft circulated for comment on 13/2/07.
Version 2 Draft B	14/2/07	As draft A, but with Sections 6 (Workplan) and 7 (Conclusions) completed.
Version 2 Draft C	15/2/07	As draft B, but incorporating: feedback from SAP, additional references, update of executive summary, completion of lists of potential post-TrustCoM functionality, minor tidying up and corrections.

Table of Content

Executive Summary

This report was initially primarily a planning document, defining the scope of the demonstrator to be produced in Work Package WP38, analysing the work required to produce it, and assigning roles to partners. It has been updated with design decisions made during the first phase of implementation, and now also serves as a description of the initial version of the demonstrator (D57). The changes primarily affect Section 4 onwards. The main output from WP38 is a prototype environment supporting ad hoc integration of services with loosely-coupled business communities (a Virtual Hosting Environment), built according to the principles of TrustCoM Framework. We summarise the concept and its application in an eLearning business context, map the abstract TrustCoM architect onto the concrete structure implied by the VHE concept, then describe scope of the demonstrator and design and implementation decisions. An explanation of the rationale for these descriptions is provided. We also outline the implementation and demonstration plan in three phases. The first phase is now completing and has resulted in the initial version of the demonstrator (D57).

An important concept to emerge from TrustCoM is the Virtual Hosting Environment (VHE). This is an implementation of the kernel of the TrustCoM framework operated by a hosting service provider as the nucleus around which communities of enterprises may form. We expect that the Virtual Hosting Environment concept will be widely taken up. It offers substantial business opportunities to service providers, especially existing operators of telecommunications networks, data centres and application hosting facilities. The existence of VHE implementations, will create opportunities for companies and other organisations to form Enterprise Networks (ENs) and other communities on a commercial or public service basis. In turn, the availability of these safe environments for co-operation will remove barriers to the blossoming of an ecosystem of innovative small companies and be a considerable stimulus to European economic prosperity. Note that BT and Microsoft are already co-operating on a network-based platform for Web2.0 mashups [10, 11]. Conceptually, the mashup is very similar to the dynamic aggregated service that the WP38 VHE is designed to support, and the popularity of Web2.0 supports our belief in the emergence of a new business model based on agile collaborations of small enterprises.

This document lays out the plan for development of an Ad Hoc Aggregated Services demonstrator derived from the corresponding testbed in AL2 and describes progress to date. The main objectives of the demonstrator are to:

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

The main sections of the document deal with the following topics:

- Explanation of the VHE concept and the business rationale for the main stakeholders, the example VO application to be used to demonstrate the concept, and the relationship to other strands of work in the TrustCoM project, principally the testbeds and reference implementation being developed in AL2.
- The high level architecture for the demonstrator. This section aims to define the basic structure of the demonstrator without prescribing the functionality in any detail. The functionality is largely provided by services deployed within the architectural framework. Selection and prioritisation of services to be deployed is considered subsequently.
- Analysis and prioritisation of VHE requirements resulting in definition of the baseline functionality to be provided by the demonstrator, and identification of the associated services. The first priority is to implement this baseline in the demonstrator. The functionality will be enhanced subsequently within the project if time allows. Note that it is intended that the partners will continue to use and develop the demonstrator beyond formal the end of the project.

- Document the scope of the demonstrator in terms of core functionality of the VHE and potential enhancements, and describe design decisions and explain the rationale for them. Topics for experiments regarding eventual integration with a next-generation, converged, multi-service network (NGN) such as BT's 21st Century Network (21CN) are also discussed here.
- Assignment of responsibilities and a work plan for the main phase of WP38.
- Conclusions and observations based on experience to date.

The main difference between the demonstrator and the AL2 AS testbed is the emphasis on the VHE concept as the basis of a network-hosted service platform. There is a clean and clear separation of the application-specific services from the application-neutral core functions composing the VHE, and to enhance realism in the demonstrator the VHE and application services are hosted at different partner sites (BT and Atos Origin, respectively). The core functions are also more closely integrated to create a prototype service platform rather than collection of components, and management interfaces are enhanced to make the demonstrator credible for eventual business use. Some of the reference implementation elements are also being 'upgraded' to more mature equivalents that are more suited for use in live business applications. One feature of the architecture is the use of the packaged gateway (including gateway infrastructure and local 'per-partner' services such as Security Token Services and Policy Decision Points) as a modular building block. One gateway is assigned to each partner in the EN making the architecture scalable and also making a clear separation between what is under partner control and what is under control the EN or a VO.

Not all the functionality available in the TrustCoM reference implementation is included in the demonstrator as planned for completion with TrustCoM. This is because one the main design objectives was to create a well-integrated, rounded basic platform containing the essential facilities required, and to which other services could easily be added. Thus priority was given to fundamental features that are useful in wide variety of contexts (the 80-20 rule), and indeed can be built upon to create some of the 'missing' functionality. The three fundamental blocks of functionality to be implemented are Fundamental Access Control, Fundamental Monitoring and Accounting, and Basic EN Membership and Central Service Management. They are described and the choices justified in Section 4.

At the time of writing, the initial version of the demonstrator is approaching completion. It consists of the baseline application services deployed at Atos Origin working in conjunction with gateways (one per partner) deployed at BT. The baseline gateways implement the 'control plane' elements of the access control functionality as the VHE infrastructure. No major technical problems have been encountered. Progress has been slower that originally planned but this is due to resourcing conflicts within the project, which will soon be resolved as other work packages complete.

A major purpose of the demonstrator is to engage with business stakeholders in TrustCoM partners, advisory board members and also interested parties outside the project. Such demonstrations will only become possible towards the end of Phase 2 when the core functionality will be in place, so it is not yet possible to report back on this aspect. We feel confident, however, that the demonstrator will be an effective vehicle for explaining and promoting the VHE business and technical concepts and also the overall TrustCoM Framework. Although the VHE is only one possible incarnation of the generic TrustCoM framework, it includes most of the fundamental technical features, and it is often easier to first explain a concrete instance such as the VHE and then generalise to other possible cases.

1 Objectives

The main objectives of WP 38 are to:

- Make progress towards commercial exploitation of TrustCoM framework
- To create a prototype platform based on the TrustCoM framework that a provider (e.g. BT) can use to offer services to VOs. This is referred to as a Virtual Hosting Environment (VHE) below
- Evaluate the potential for integration with service oriented 'capabilities' exposed by IP-based Next Generation Networks (NGNs), e.g. BT's 21st Century Network (21CN)
- Show commercial potential via a convincing example application

This report was originally primarily a planning document, defining the scope of the demonstrator, analysing the work required to produce it, and assigning roles to partners. It has been updated with design decisions made during the first phase of implementation of the demonstrator, and now also serves as a description of the initial version of the demonstrator (D57).

The remainder of this section outlines:

- the VHE concept and explains the business rationale for the main stakeholders
- the example VO application to be used to demonstrate the concept
- the relationship to other strands of work in the TrustCoM project, principally the testbeds and the reference implementation of the TrustCoM Framework being developed in AL2.

1.1 Virtual hosting environment

In the modern business world, the boundaries between enterprises are becoming less distinct. Facets of this trend include:

- consortia being formed to provide services beyond the capability of individual members
- outsourcing to allow companies to focus on core competences
- use of utility computing, hosted data centres, 'software as a service' / hosted applications
- cross enterprise business process integration and electronic processing of business to business (B2B) transactions
- extended supply chain integration including use of electronic market places

While often these are justified in terms of decreasing cost, in reality the need for business agility resulting from automated service interconnection and information exchange is if anything more important.

Virtual organisations (VOs) represent the extrapolation and convergence of these trends, enabled by open standards-based technology including web services and grid computing. A Virtual Organisation is a temporary or permanent coalition of geographically dispersed individuals, groups, organisational units or entire organisations that pool resources, capabilities and information to achieve common objectives.

In addition to VOs that are more agile and dynamic versions of traditional business partnerships and consortia, we also envisage the emergence of new forms of business collaboration that could not exist without the new generation of open standards-based technology. In particular, we are interested loosely-coupled, geographically dispersed communities of individual knowledge workers and innovative small businesses. Many believe that innovative small businesses will be the engine for future economic growth in Europe. However, individually such businesses lack the scale and breadth to compete with large enterprises. Visionary scenarios have been proposed (e.g. [1][2][3]) in which small business / individuals with complementary capabilities are able to cooperate flexibly, supported by appropriate new technology, to provide a range of services currently only within the scope of large corporations. Indeed businesses have founded based on this type of model (e.g. Elance [4], guru.com [5], hotdispatch.com [6]]).

A new economy based on Virtual Organisations requires an environment within which businesses can quickly come together to share resources and work together to achieve the project goals. The negotiation, monitoring and enforcement of contracts and agreements that takes into account reliability, accounting, security and other issues such as IPR will be an important component of this environment. In addition, there is a requirement for services to replace the trust inherent in operation within an integrated real organisation (trust in colleagues - even when not known personally, trust in procedures and processes, etc.), and the trust between customer and an established service provider with a clear legal identity and brand / reputation.

In long-lived, stable collaborations, bespoke implementations of the TrustCoM framework may be designed and constructed to meet specific requirements. However, creation and operation of shorter-lived, dynamic VOs cannot be done in this way. We envisage service providers such as BT operating platforms that provide the core infrastructure and functions of the TrustCoM framework fully integrated with underlying network capabilities. We refer to this as a *virtual* hosting environment (VHE), because in the typical case the ICT system supporting the operation of the VO federates VO partner systems and the VHE itself, which acts as a hub, providing central services and connecting the partners together.

For the foreseeable future, it seems unlikely that VOs will be able to form rapidly without some pre-existing contractual, commercial and technical framework for co-operation. Within TrustCoM we are using the term Enterprise Network (EN) to refer to a community of companies – typically operating in a particular industry or application domain - that is bound by agreements, conventions and procedures that facilitate the formation and operation of VOs by the EN members. Thus, the VHE supports two levels of community: the EN, being an 'ecosystem' of entities willing and able to form VOs, and the VOs themselves, many instances of which may co-exist within an EN.

For simplicity, we assume that a VHE hosts a single EN[1] (i.e. that). In the case of ENs corresponding to stable business partnerships, the VHE may support a consortium with an organisational structure and established business and trust relationships at a high level. The VOs are then specific ventures or projects undertaken by the consortium or subsets of the companies within it. Although such a consortium could establish its own collaborative infrastructure, there are still advantages in separating distinctly the support for collaboration from the internal operations in the form of a VHE operated either by the consortium or by an impartial, trusted entity. In contrast, where an EN is a loose-knit dynamic community of companies, some form of VHE is not just advantageous, but is clearly essential.

The virtual hosting platform is essentially an 'unpopulated'[2] instantiation of the TrustCoM framework, including the infrastructure layer (which can be thought of as a message bus that can be configured dynamically to enforce security and other policies), subsystems dealing with adaptive, policy-driven trust and security, SLA monitoring and enforcement, and VO Management. The VO Management services capture and utilise the agreements, partner roles and business processes at both the EN and VO levels. In the SME-based scenario, VOs are very dynamic and must form and operate automatically. To make this possible, much of the preparatory work must be done in advance, typically when the EN is formed or when a new member joins. At EN formation time, framework VO agreements and organisational and business process templates must be established so that VO-specific agreements and templates can be instantiated on demand by specialising the framework agreements and templates. As part of the negotiation to join the EN, members have to achieve a degree of qualification by satisfying certain requirements, and to have made certain commitments. Consequently, proof of EN membership provides evidence of trustworthiness. Subsequent behaviour of EN members is monitored, and a poor track record may eventually lead to exclusion from the EN.

The most fundamental function of the VHE is to enact policies monitoring and policing agreements at the VO and EN levels. Because partners are autonomous organisations and retain control of their own services and resources they cannot be forced to fulfil commitments. Rather the VHE:

- Provides facilities to enable partners to meet their commitments without compromising their own security and other interests.

[1] One can envisage VHEs that can host multiple ENs, maintaining complete or partial separation between them in the manner of virtual private networks. This adds quite a bit of complexity, so we assume here that a separate VHE instance is set up for each EN.

[2] i.e. it needs application services, meta-data, etc. to complete and customise it.

- Blocks activities that are not consistent with agreements
- Detects violations of agreements and presents this information in a form that facilitates the appropriate action being taken.

The infrastructure layer, for which BT has primary responsibility forms the basis of the VHE platform and holds the key to providing its core functions. It enables those web services that the EN members have made available to communicate with each other under highly controlled and VO context specific circumstances. It is essentially a SOAP message bus that is highly configurable and into which a variety of enforcement and monitoring elements can be deployed. These elements act on messages passing across the infrastructure performing operations such as routing, verification and validation, transformation (e.g. credential chaining), and monitoring / logging / reporting. The order of operations and detailed behaviour of the elements is under the control of rule-based policies that may themselves be modified in response to observed behaviour.

The table below enumerates the main stakeholders in an EN hosted by a VHE and the advantages for them of the VHE concept in comparison to a bespoke EN infrastructure. Note that the roles are relevant to the current scenario, in which the EN is long-lived collaborative entity, and VOs are transient communities forming within it.

Stakeholder and description of role	**Business advantage of VHE**
VHE operator the entity hosting the enterprise network and providing re-usable infrastructure and core services	This is a new business role, though related to application and data centre hosting. For a NGN operator such as BT, it is an opportunity to leverage existing network infrastructure to provide added value, higher margin services. There is a high degree of synergy between the VHE concept and the move to a service oriented approach to exposing generic network 'capabilities' taken by some network operators.
EN founder (or initiator) the entity running the EN. It may also be a service provider/consumer within the EN. It is similar to the VO initiator in other TrustCoM scenarios.	This is assumed to be an entrepreneurial entity or one motivated by a wish to serve or promote the formation of a co-operating community. It is likely that such an entity would have problem domain knowledge or business expertise as its core skill. Existence of a VHE would enable it to launch and operate an EN with little capital investment. It would also require relatively little technical expertise (though this depends to some extent on the facilities provided by the VHE operator).
EN member a service provider and/or consumer within the EN community	The VHE concept allows the EN members to outsource the support for co-operation. The outsourcing occurs at several levels. The most basic is that of the infrastructure for secure and trusted interoperation of services with other VO members. In addition, integration of the VHE platform with an underlying 'capability-oriented' NGN infrastructure would allow member services to draw upon a wide range of network-based services (e.g. billing platforms).
External consumer an entity external to the EN benefiting from services provided by VOs formed within the EN. This could be an employee within an EN member company or an external customer.	Benefits from increased confidence in the services provided by the EN. Not only is there more confidence in the technology, but trust is to some extent inherited from the VHE operator's brand. Integration of the VHE with the underlying network platform is likely to give a more seamless experience – consuming services provide by the EN is little different for consuming other services from or hosted by the network operator.

1.2 Demonstration scenario

A typical SME-based scenario would be the following: An operator (say BT) offers a ('virtual') hosting service to SME enterprise networks, i.e. it is the VHE operator and hosts kernel services to which the participating SMEs federate their resources (see Figure 1). A customer organisation approaches BT with a view of establishing an SME EN in a particular business domain (say). The EN is 'instantiated' with an initial core

membership (maybe just the founder) and opened for business. SMEs approach the EN management to join the EN. The joining process involves various things like federating the new SME's platforms with the EN core platform, agreeing to contracts, registering services, and so on. A customer comes along with a particular requirement, and a set of partners and services are selected from within the EN community, etc. The VO is formed and interacts with the customer to agree and deliver services.

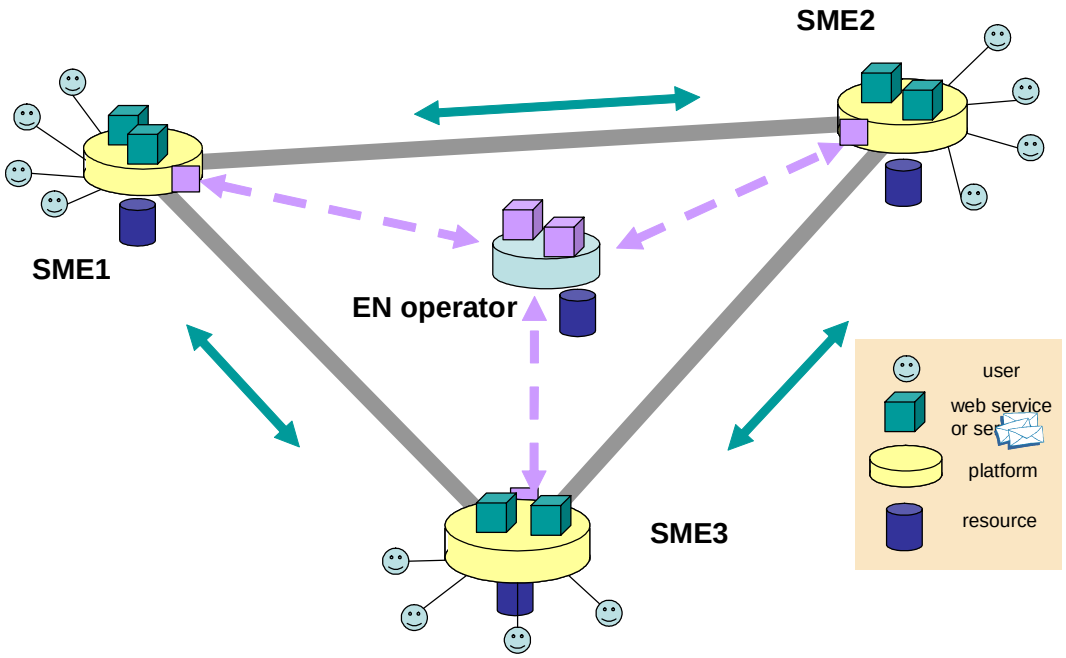

Figure 1*: An EN operator provides kernel services for an SME Enterprise Network*

We have selected eLearning as an example business domain for the enterprise network. The main categories of partner in the eLearning EN are:

• **Training Consultants** – TCs interact with end-users to understand their training requirements and formulate them in a way that may be used to construct a personalised training programme.

• **Training/eLearning providers** – these act as integrators, building bespoke training packages and co-ordinating their delivery to the end-user

• **Content providers (aka Learning Resource providers)** – these modular resources that may be used with training packages

• **The eLearning EN operator** – provides additional services such as a specialised portal, payment services via banks, etc. as well as generic services supporting trust, security and contract management in the operation of the VO.

Relative to the roles tabulated earlier, all of these are EN Members. The eLearning EN operator has the special status of EN founder. The people requiring training are the external consumers.

A typical use case might go as follows:

The end user accesses the portal and selects a training consultant. This might be one the user has an existing relationship with, or might by one specialised in a particular topic or in a particular category of user. The training consultant interacts with the user to obtain training requirements, then issues an invitation to selected training providers to offer bespoke course that meet the requirements. The training providers respond with programmes constructed from modules offered by various content providers. Advised by the training consultant, the user selects an offer from one of the training providers. The selected training provider coordinates the delivery of the training as required by the user. The training consultant may maintain an involvement in this phase to monitor the user's progress and advise on changes to the programme. At the

end of the course payments are distributed to the various service providers subject to user satisfaction and fulfilment of obligations.

Challenges for trust, contract and security management inherent in this scenario that are addressed by the TrustCoM framework include:

- **Trust Management**: it is possible that training consultants may have to rely on training and content providers with whom they have never had experience. Consider, the end-user may require a course that was not previously part of the consultant's portfolio of experience. In order not to lose their credibility with end-users (i.e. their clientele) they will require mechanisms for evaluating the reputation of selected providers, according to available attributes and set criteria.
- **Contract Management**: it is expected that the provision of services will be associated with service level agreements (SLAs), such that the registration and monitoring of these SLAs needs to be supported in the infrastructure, by consultants and by providers. For example, in order to maintain consistent, reliable learning services, providers may have agreements over service availability and response time.
- **Security Management**: it is necessary to have a comprehensive set of mechanisms for access control to management and support services as well as to application services. It is desirable to have a uniform mechanism for supporting both aspects of access control. For example, the EN operator will want to limit access to the portal services to EN members, while each provider will want to limit access to their context and services to VO members with whom they need to interact.

Note that the short-lived and ad hoc nature of the VOs in this scenario mean that the above challenges must be met using mechanisms that provide business agility through automated interconnection of services and information exchange.

1.3 Relationship to AL2 testbeds and reference implementation

The WP38 demonstration of the VHE concept and an associated example application draws upon results from elsewhere in the TrustCoM project, and in particular on software modules developed within AL2. It is important to realise, however, that the WP38 demonstrator is not simply a development of the corresponding AL2 testbed. Whereas the AL2 AS testbed is an experimental prototype used to illuminate the requirements for the TrustCoM framework and evaluate its incarnation in the reference implementation, the WP38 demonstrator is focused on demonstrating a commercial concept (the VHE) enabled by the TrustCoM framework and making progress towards a pilot implementation of the concept usable in business trials. This difference has a number of implications, including the following:

- There is no commitment to including the whole of the reference implementation functionality in the demonstrator. Selection of which sub-systems and services to include is based on: a) importance of the functionality to the VHE concept, and b) maturity of the current implementation. In considering the importance of the functionality, priority is given to essential functions without which a VHE would not be considered useful, and fundamental mechanisms upon which higher-level functionality can be built. The rationale for the second criterion is that the VHE platform could be extended after the end of project if the fundamental mechanism are in place. Note that a distinction must be made between use of the TrustCoM Framework and use of components from its reference implementation. A decision not to use all available elements of the reference implementation, either because the functionality is not required for this application or because an off the shelf substitute provides adequate functionality in a more robust embodiment does not mean that the TrustCoM framework has been abandoned.
- Development and enhancement of the TrustCoM reference implementation components falls within the scope of AL2. Software development effort in WP38 will be required for customising and integrating additional components from outside the TrustCoM framework that are required for the VHE concept. Selection decisions regarding whether to incorporate a TrustCoM component into the demonstrator take into account functionality, completeness and robustness.

2 High level architecture

This section aims to define the basic structure of the demonstrator without prescribing the functionality in any detail. The functionality will largely be provided by services deployed within the architectural framework. Selection and prioritisation of services to be deployed will be considered in Section 3.

The relationship view of the architecture specified in TrustCoM Framework [1] defines the following logical categories of service in addition to the application services:

- VO Management
- BP Enactment
- SLA Management
- Policy Services
- Trust and Security Services
- EN/VO[3] infrastructure

The framework permits many variations regarding:

- What services within these categories are instantiated and in what form
- How the service instances are deployed over partner and third party sites. Since the default mode of communication among these services is via SOAP messages, many options are available here.

This section is concerned with defining the basis of a deployment architecture in terms of:

- (partner and third party) sites and how they are interconnected
- general principals regarding how instances of the various categories are to be deployed across this architecture.

Section 3 will consider the service instances to be deployed within this architectural framework.

2.1 Abstract high level architecture

Recall that the VHE scenario has the following main players:

- a number of providers and consumers of application services. These are members of a particular EN, and hence candidate members of VOs formed within it. In the specific demonstration application adopted here, the EN is a community of providers of eLearning services.
- An EN 'founder', being the entity that runs the EN as a business. This entity may or may not also be a service-providing member of the EN. It typically has domain-specific expertise, e.g. concerning eLearning.
- The VHE operator, that hosts the EN, in the sense of providing application neutral services that enable the domain-specialist EN founder to manage the EN in conjunction with the ordinary EN members.

We consider each of these main players to operate one or more 'sites' (exactly one unless otherwise specified). In reality, the EN members may or may not use a third party to host their site, and this third party may or may not also be the VHE operator.

Consistent with the TrustCoM architecture, we consider each of the sites to be linked and protected by one or more (exactly one unless otherwise specified) TrustCoM gateways. These host services performing a number of functions including:

[3] 'the EN/VO' is used here as a short-hand for 'the EN or VOs formed within it as appropriate'.

- credential conversion
- enforcement of access control and other policies
- monitoring / event logging and notification
- encapsulation and virtualisation of services

To a first approximation, this network of gateways is what is referred to in the TrustCoM framework as the EN/VO infrastructure. As is common for entities at the boundary between network infrastructure and customer sites, the gateways could in principle sit within the network, be part of the customer's own facilities but conform to standards accepted by the network, or be 'customer premises equipment' owned by the network but located on the customer site. In the case of the current demonstrator, we consider them to be sites of a specialised kind, and that in the normal case they are owned and operated by the VHE operator, but with certain management rights delegated to EN members. The rationale for selecting this configuration as the normal case is that locates all TrustCoM specific aspects of the architecture under the ownership of the VHE operator (for whom it is a re-usable asset) and hence minimises capital investment and disruption for the partners and also time to set up a EN.

This overall situation is shown in Figure 2. The distinction between the two VHE operator-hosted EN Central Management sites will be clarified later. The sites with names beginning 'GW' are gateways. The gateways labelled GWVM and GWTTP may be omitted in some variants because the two sites the are associated with have a more trusted status. Consequently they are shown faded and with dashed borders.

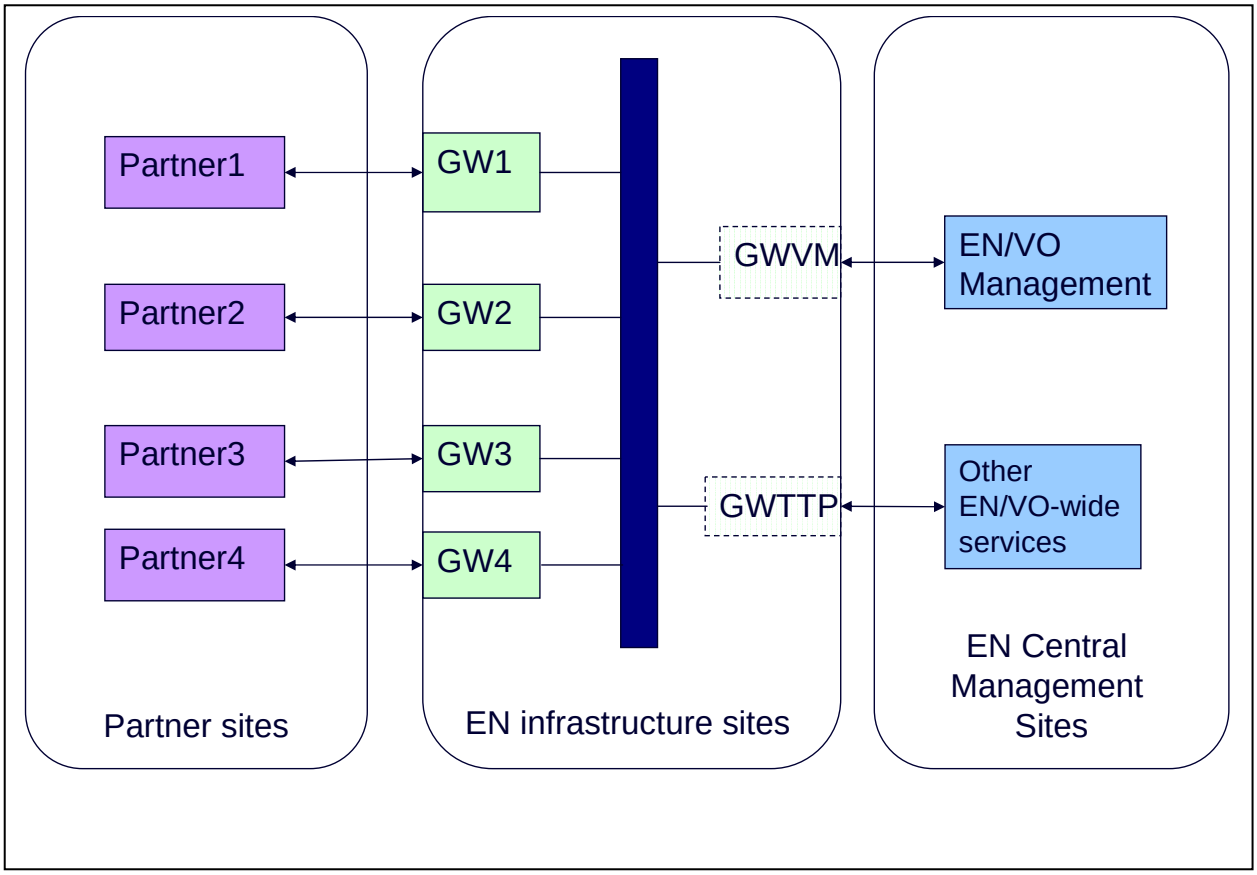

Figure 2: Abstract testbed architecture

2.2 Demonstration platform architecture

The concrete architecture for the demonstrator reflects the abstract testbed architecture shown in Figure 2 in quite a literal way. Each site will normally be represented by a computer or collection of related computers, though in some cases multiple sites may be represented by distinct logical partitions / containers within a single computer. Each computer will normally run one or more web service containers allowing partitioning of services within the 'site'. 'Container' is used here as a generic term to refer to a web service deployment platform such as and instance of TomCat/Axis, the equivalent under the .net framework, BEA WebLogic or other such software. Other more specialised software (e.g. web service gateway software) may also be run by some of the computers.

The initial assumption is that the main host locations for the demonstrator will be BT at Adastral Park, Ipswich, UK, and Atos Origin, Barcelona. In the default case, BT will be responsible for the integrating the gateways and will also host the master network of gateway 'sites'. It is expected that BT will also host the computers representing the two EN Central Management Sites. Atos Origin will be responsible for the partner sites and host the master copies of them. However, there are advantages in having the full demonstrator replicated[4] at both sites. Advantages include: simplifying the integration and testing process, enabling demonstrations independent of internet connections, continued availability of demonstrators.

Variations on this will also be considered, specifically the following possibilities:

- A different partner may host one or both of the EN Central Management sites (e.g. SAP could host the EN/VO Management site)
- One or more of the gateways may hosted by Atos to represent the case where the gateway is sited on customer premises.
- One or more gateways may be technically dissimilar and hosted by Atos to represent the case where an EN member provides its own gateway.
- One or more EN member sites may be hosted at BT to represent the case where application hosting is outsourced to a hosting service provider who is also the VHE operator.

2.3 VHE architecture

We now consider in principle how the TrustCoM services are mapped onto the VHE architecture, without at this stage making a commitment to use of particular services in the demonstrator or to use of particular technical platforms.

As a preparatory step, it is useful to follow the practice adopted in telecommunications network architectures and distinguish between data, control and management 'planes'. The data plane is concerned with actually delivering the services. It contains the providing and consuming application services and the data paths that connect them, typically via intermediate nodes. The control plane is concerned with controlling the way the services are delivered and ensuring that they are delivered. It contains signalling data flows between local control elements associated with the intermediate nodes. The management plane is concerned with overseeing the operation of the network and communicating policy and configuration changes to the control plane entities.

Applying this model to the TrustCoM architecture, the data plane consists of the application services and policy enforcement points (see Figure 3). The control plane (see Figure 4) contains token services, policy decision points, and analogous services in the SLA Management and BP Enactment sub-systems, for brevity, these are referred to as policy decision services in the figure. The management plane contains EN/VO Management-related services (see Figure 5). In each of these three planes we can distinguish between elements that are under the control of EN/VO members, those that are under the control of the EN/VO or its management, and those that sit on the boundaries between the zones of influence of the partners and the EN/VO (see Figure 6).

[4] These may not be exact replicas if there are constraints due to e.g. licensing and use of local resources.

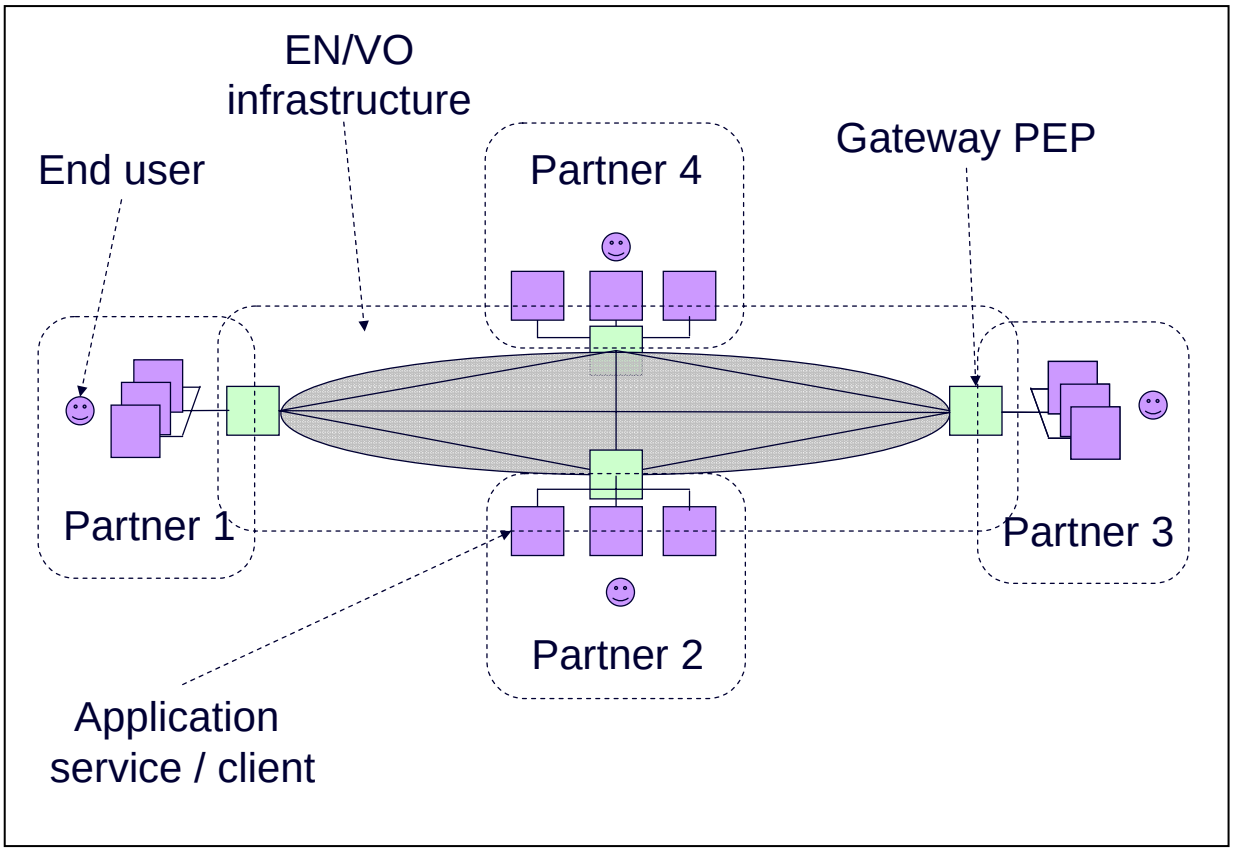

Figure 3: TrustCoM data plane

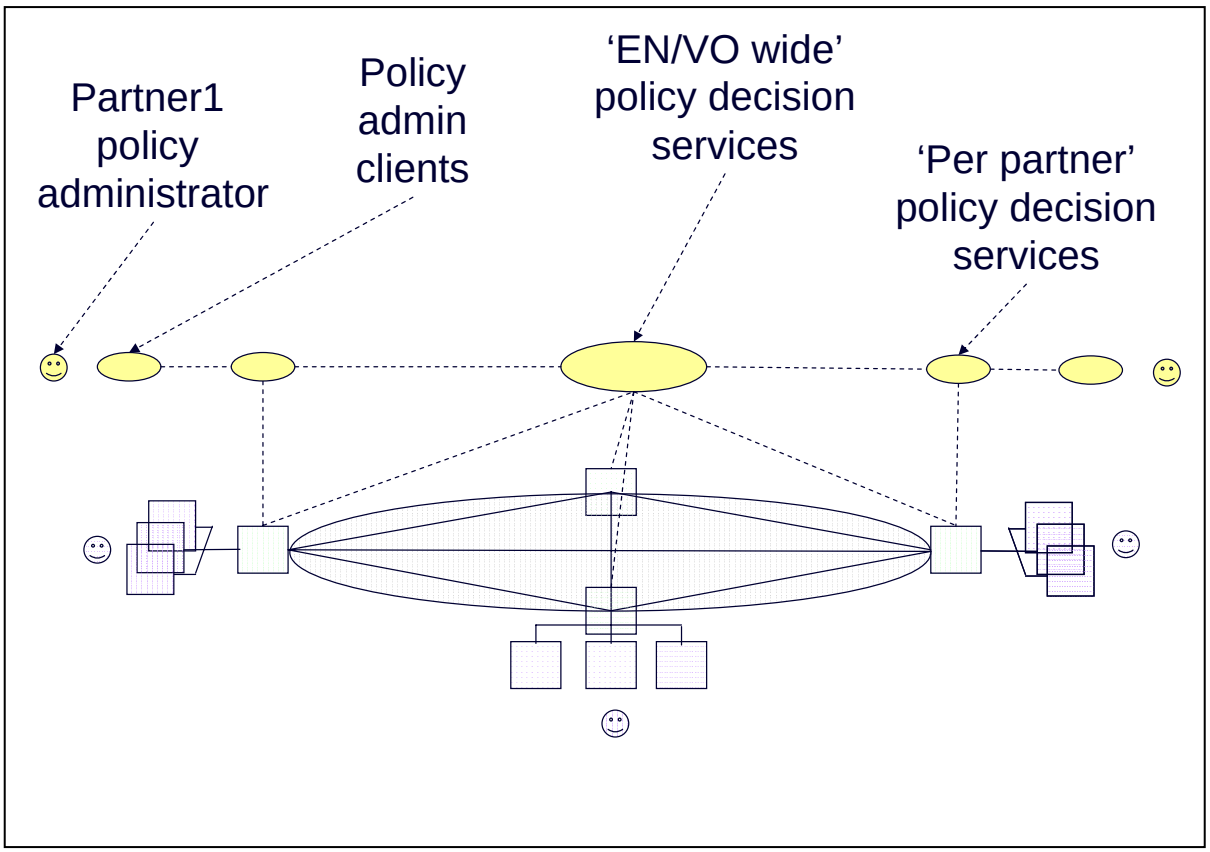

Figure 4: Adding the TrustCoM control plane

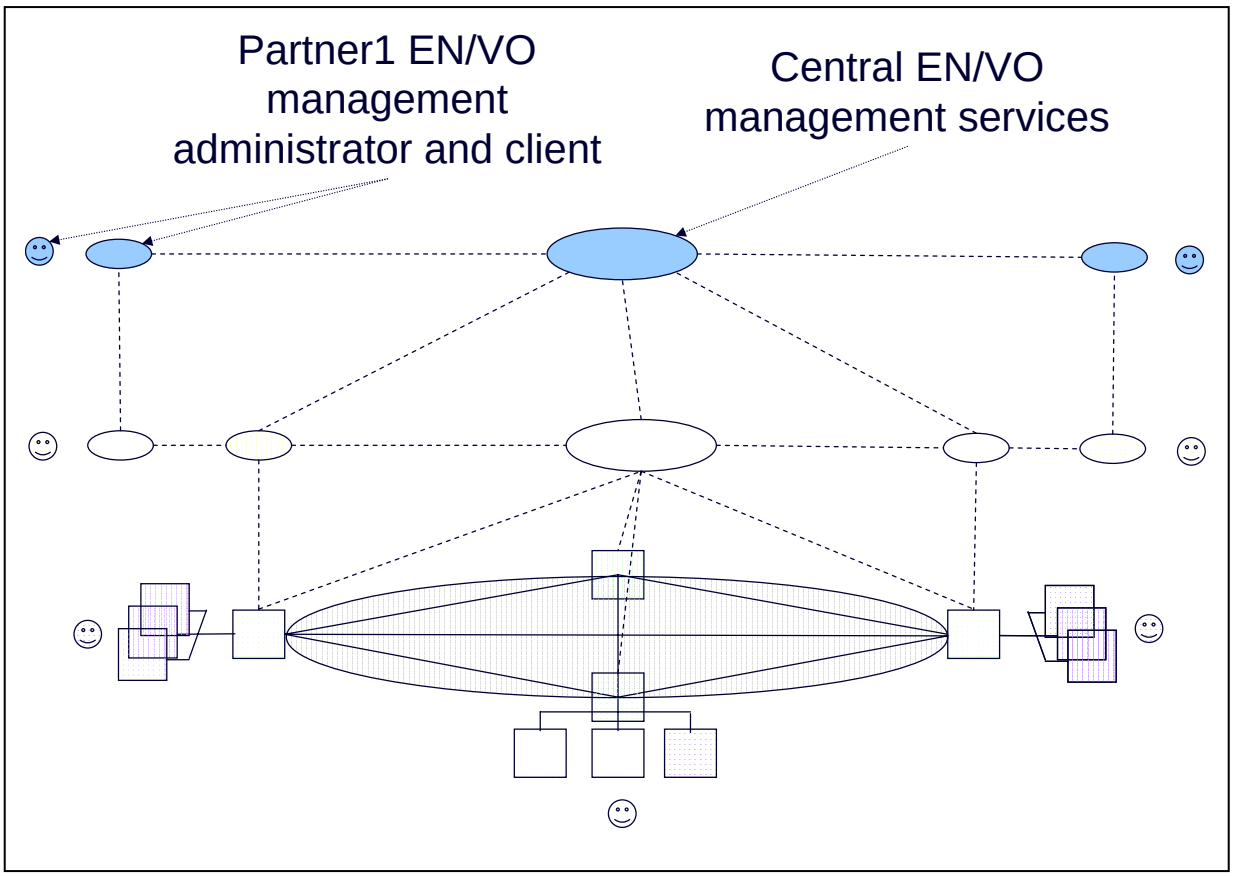

Figure 5: ... and then the TrustCoM management plane

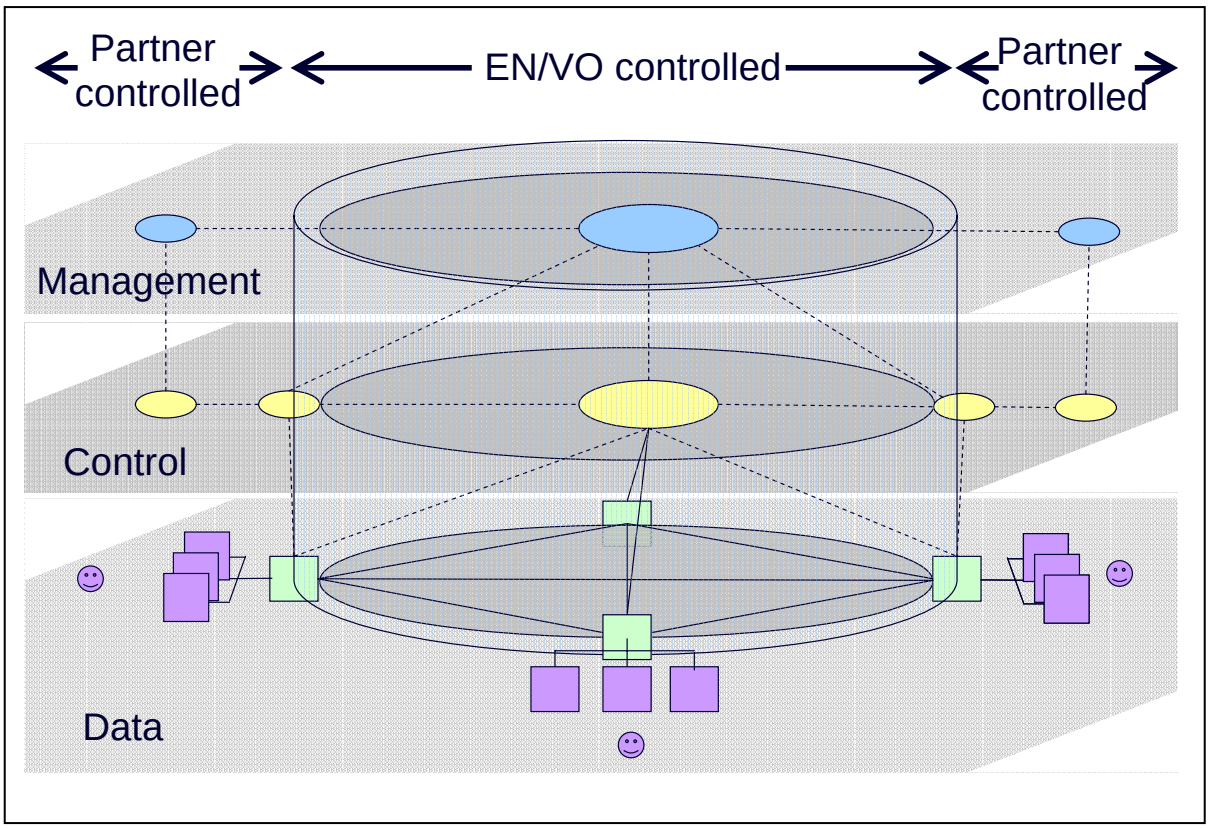

Figure 6: The stacked TrustCoM planes

The VHE demonstrator platform consists of the servers representing the EN infrastructure sites and EN Management sites shown in Figure 2. We consider each of these sites to be partitioned into a number of logical containers to allow a clear distinction between different classes of service deployed on them. As a general guide, a gateway consists of a PEP plus containers for types of per-partner 'policy decision' services; the EN Management site has one or more containers for central EN/VO management services; and the site for 'other EN/VO-wide services' has one or more containers for types of EN/VO-wide control plane services. Note that within TrustCoM, the EN/VO-wide control plane services are often referred to as TTP services, and for brevity, this term will be used below. The control and management plane clients are closely related to the VHE, but hosted in compartments in the partner sites. In practice, in many cases these will be browser-based thin clients, with the real content actually being hosted by the corresponding VHE service.

The following paragraphs go into this mapping of service instances to containers within sites in a little more detail. Note that some of this account depends on interpretation of aspects of the TrustCoM architecture that are still fluid.

2.3.1 Gateway site

We partition each gateway site into logical 'containers' as follows:

- Policy Enforcement container (PEC) hosting/implementing the following
  - Configurable Policy Enforcement Point (PEP)
  - A repository into which can be loaded chainable enforcement and monitoring elements (often referred to as handlers or interceptors) to make them available for use by the PEP
  - An Instantiator, responsible for automating service provisioning tasks

  - A Notification component providing local services implementing aspects of the EN notification capabilities.
- One or more containers hosting generic (i.e. application neutral) TrustCoM services that are provided on a 'per-partner' basis. Examples include:
  - Security Token Services (STSs)
  - Policy Decision Points (PDPs)
  - Event-Condition-Action (ECA) policy service if required on a per-partner basis
  - VO context management
  - a local service registry
  - Various services comprising the per-partner constituents of the TrustCoM SLA monitoring sub-system
  - Per-partner BP engines (if provided or hosted by the VHE_
- A container able to host application or partner-specific service within the Gateway server where this is required or convenient.

2.3.2 EN/VO management site

This consists of one or more logical containers hosting services concerned with management of the EN or VOs within the EN, for example:

- VO Lifecycle Manager
- Membership manager
- GVOA Manager
- Management plane services of the BP Enactment sub-system
- Management functions of the SLA sub-system (SLA manager, SLA Evaluator, SLA negotiator, SLA repository, etc.)

2.3.3 TTP server

This consists of one or more logical containers hosting generic services used in the operation of an EN or its VOs, that are required on a 'per-EN' or 'per-VO' basis. They may be provided by the VHE operator, the EN founder or by independent parties. Examples include:

- EN-wide STS, PDP (if required), EN-wide ECA policy server
- EN-wide control plane services of the SLA and BP Enactment sub-systems
- Central audit log service
- Reputation service

2.3.4 Inter-gateway communication

This could be implemented in a variety of ways, from straightforward SOAP over HTTP to using an enterprise message bus product based on message-oriented middleware. The implementation mechanism is hidden from the EN partners. Furthermore, any implementation-specific aspects of the gateways will be minimized and confined to well-defined, replaceable or configurable modules.

2.3.5 Management and control clients

Partners need to interact with the VHE for a variety of purposes, including:

- Deploying / provisioning services to make them accessible within the EN
- Negotiating membership of EN/VOs and terms of GVOAs
- Changing access policies and SLAs

Each of these purposes requires some form of client, typically either

- A web browser interface via a management portal provided by the VHE
- A web service client provided by the VHE but hosted by the partner
- A web service client provided and hosted by the partner, but conforming to an interface specification provided by the VHE.

2.4 Application

The application used in the WP38 demonstrator is derived from the AL2 AS testbed, which implements a simplified version of the scenario described above in Section **Error! Reference source not found.**. The EN founder operates an eLearning portal providing end-user access to learning services. The portal operator also acts as the single training consultant and training provider in the EN, and the training consultant and provider software is integral to the portal. The other EN members are learning resource providers (LRPs). We thus have:

- One server belonging to the portal operator and hosting the eLearning portal and its constituent services. End users interact with the portal via a browser interface. There is a back-end to the portal that implements a web service interface for communication with other partner services via its VHE gateway.
- Two or more servers belonging to partners in the LRP role and hosting services providing access to learning resources (i.e. course modules).

3 Analysis and prioritisation of VHE requirements

The VHE requirements can be characterised using two main dimensions:

1. Trust, security and contract management functionality provided to hosted EN/VOs.
2. Functionality provided to facilitate management and administration of the above-mentioned functionality and of the EN and VOs.

In both cases, we can rank the functionality from the most basic and fundamental, to the most sophisticated and elaborate, with the most fundamental being accorded the highest priority. An important factor in establishing this ordering is the existence of dependency relationships: a service upon which other services depends, being considered as more fundamental than the dependent services. Since the management functionality is of no use without the services it is used to manage, the second dimension is in this sense, subsidiary to the first.

We restrict ourselves here to considering support for a 'Basic' EN and associated VOs as typified by the eLearning application. The first part of this section outlines the main features and requirements of such an EN. The following parts analyse the basic level of functionality for each class of requirement. These are presented in approximate order of priority.

3.1 Analysis of generic application

This application is in fact an example of a common pattern found in e-commerce applications of web services: the end-user interacts with a front-end portal; the portal interacts with one or more back-end web services, selecting and combining them as appropriate to suit the end-user's requirement. The VHE should be independent of the specific application, and also extendable to more complex forms of EN. Consequently, we will try to generalise the requirements as far as possible without introducing unnecessary complication.

The following simplifying assumptions are made to ensure implementation of a demonstrator is feasible in the time available:

- There is a degree mutual trust among EN members. This is justified if some form of qualification test is required to join the EN, and if membership is withdrawn for untrustworthy behaviour.
- The EN membership agreement is standard across all members and has standard provisions covering all VOs within the EN. It provides a framework agreement upon which VO agreements are closely based.
- One standard provision is that no EN member may unreasonably refuse to provide a service to another. An example of an acceptable reason to refuse is shortage of capacity due to prior commitments.
- Management of end-user identities is the responsibility of the relevant EN member rather than the EN itself. Each end-user is associated with one of the EN members, e.g. as a customer or as an employee. End-users of the EN as a whole, for example a customer of the eLearning EN which returns periodically to purchase new training, may be associated e.g. with the EN Founder / portal operator. Guest / temporary accounts may be used for casual end-users.

Major (coarse grained) use cases include:

- Founding / disbanding of the EN
- Member joins / leaves the EN
- Member registers / deregisters service with EN
- Member sets / modifies SLAs and policies associated with a service
- End-user registers / de-registers with a member

- End-user selects and requests composite service and a VO is formed in response
- Fulfilment of a service in the context of a VO
- Assurance of a service in the context of a VO
- Generating events upon which billing for a service in the context of a VO can be based
- Dissolution of a VO

In all of these there is a choice as to whether support is provided by the VHE, by the application services, or by some 'out of band' mechanism. The following sections describe in rough priority order, the candidates for support by the VHE.

3.2 Fundamental access control

3.2.1 Context

In principle this applies to any message exchange within the EN. It is fundamental to EN security.

3.2.2 Description

The most fundamental requirement is for basic access control in the context of simple transactions. This corresponds approximately to Scenario 3, Phase 1 in AL2. Following a message through from source to destination, it involves:

- At source gateway: Egress control, logging, mapping of credentials from source partner domain to EN/VO domain, addition/conversion of tokens.
- At destination gateway: Access control, logging, mapping of credentials from EN/VO domain to source partner domain, validation/ conversion of tokens.

In addition, basic session control is required to relate messages within the same transaction and avoid unnecessary repetition of expensive operations.

3.2.3 Required services / components / data resource

- Configurable PEP
- Chainable elements implementing required enforcement and logging operations
- Per-partner and EN/VO-wide STSs
- Per-partner and EN/VO-wide PDPs
- Local and/or central service (and user) registries
- Basic EN/VO membership directory
- Policy rules for PDPs and data resources for other services

3.2.4 Related management use cases

All require appropriate client software or portal-based equivalent, plus other services/components where specified.

- Partner modifies egress or access control policy, or logging/notification policy.
- Partner changes role assignment of personnel. End-user enrols with / cancels membership of portal.
- Partner deploys new service. Requires instantiator if provisioning is done automatically

- VHE operator deploys new enforcement element
- EN founder modifies EN-wide policies
- New VO is instantiated

3.3 Fundamental monitoring and accounting

3.3.1 Context

The ability for the VHE to act as an impartial and authoritative source of information on significant events is very important to its role. In principle these could be any events detectable by observing message traffic or other activity within the VO. Examples include messages or registry content changes that signify significant events in the lifecycle of transactions, agreements or VOs. Important categories are:

- Billable events
- Events corresponding to binding commitments, fulfilment of a service, payment, etc.
- Violation of SLAs and other commitments

This functionality is related to the TrustCoM SLA Management sub-system, but both more general and more basic. Note that the current implementation of the TrustCoM SLA Management sub-system covers basic event generation analysis and monitoring services for a restricted class of SLA Management scenario and also the corresponding higher-level services. The basic services referred to here would e.g. have the capability of monitoring certain types of derived parameter and generating events if acceptable limits were breached. They would not 'know' whether the limits were to do with an SLA, and would also be usable for other purposes. Furthermore, basic functions unrelated to SLA Management are also envisaged.

It is also related to the notification capability. It is intended to embrace the capability to instruct the PEP and other services to generate records of primitive events and send them (typically via the notification service).

The 'fundamental' capability is:

- to be able to capture primitive events and forward them to services that process and/or aggregate them and store the results for use by other services. This is essentially the TrustCoM Notification function plus mean of specifying and trapping the primitive events ('sensors').
- A number of basic services to perform some relatively generic storage and processing/aggregation functions, e.g. correlation and aggregation of primitive events to generate higher-level events, logging for audit, SLA compliance monitoring, conflict resolution, forensic and/or billing purposes.

Note that the *fundamental* capability is not concerned with how the aggregated and logged events are used by higher-level services, e.g. for SLA enforcement, billing, etc., though some examples of these would be useful for demonstration purposes.

3.3.2 Description

This makes use of similar mechanisms to those used in access control. As messages pass through the gateways events can be triggered and forwarded to analysis, audit logging and other services, or indeed to partners, by the notification sub-system. Note that many significant events can only be detected by monitoring *sequences* of messages. This is typically dealt with by sending low level events initially to a local aggregator, which later forwards the correlated composite event as appropriate.

Clearly, the gateways can only generate events based on messages passing through them and their content. There is therefore also a requirement for event generating mechanisms to be built in to certain services. Preferably this should be done in such a way that generic capabilities can be 'mixed in' to services or deployed as agents.

3.3.3 Required services / components / data resource

- Configurable PEP as for access control
- Chainable elements implementing required monitoring and event generation functions
- Reusable/deployable event generating functionality for services
- Notification mechanism
- Basic services to be decided such as audit logging, event analysis and storage for use by SLA monitoring, billing, etc.
- ECA policy service (listed for completeness – it is not clear whether ant ECA policy service is required on a per-partner basis)
- Basic derivatives of other services from the SLA sub-system

3.3.4 Related management use cases

- Partner modifies policies governing events to monitored and how they are processed
- EN founder modifies monitoring policies
- Partner deploys new service
- New VO is instantiated
- New EN-wide monitoring / analysis capability deployed

3.4 Basic EN membership and service management

3.4.1 Context

This primarily covers a collection of services allowing members and potential members (including as a special case the Founding partner) to interact with the EN as an entity. In most cases, changes to the EN, reflected in the data structure representing it in the VHE, will need to be propagated to the policy servers etc. governing the behaviour of the access control and monitoring and accounting functions. For the purposes of the initial VHE prototype, the scope is restricted to basic membership management including capture of information on contributed services and the templates allowing instantiation of VOs. The amount and nature of information captured will be determined by the requirements of the access control and monitoring and accounting functions.

3.4.2 Description

Thus is envisaged as a simplified version of the relevant services and sub-systems of the TrustCoM framework. EN members interact with a collection of management tools to update a model of the EN consisting of the following main elements:

- A representation of the EN as a collection of partner enterprises
- A basic framework agreement (GVOA) laying down rights and responsibilities of partners, etc. It is possible this could be a static, standard document that is not updated.
- A collection of templates that can be instantiated when a VO is created.
- A repository of records corresponding to instantiated VOs
- A directory of services provided to the EN by partners (and by the VHE)

Relevant changes to these must be cascaded to the policies servers etc. governing the behaviour of the access control and monitoring and accounting functions.

3.4.3 Required services

Simplified and adapted versions of the VO management sub-system and associated services

3.4.4 Related management use cases

- Founding / disbanding of the EN
- Member joins / leaves the EN
- Member registers / deregisters service with EN
- Instantiation / dissolution of a VO

3.5 Possible extensions

The above sections deliberately specify only the fundamental foundations of the VHE, a basic set of capabilities built on the foundations, plus services required for management of these capabilities. Subjective judgment has been used to decide what to exclude from the basic set of capabilities. For example, it was decided not to include a business process co-ordination mechanism as a VHE capability because this could be integrated into the eLearning application services or provided as a service by a partner. This and other TrustCoM services are candidates for inclusion at a later date. The following lists are a first attempt at prioritization.

3.5.1 First generation of extensions

- Higher-level capabilities using the Fundamental monitoring and accounting functionality, e.g. SLA enforcement
- basic BP enactment
- adaptive policy management

3.5.2 Second generation of extensions

- Advanced VO management
- Advanced BP enactment
- High level GVOA and SLA management, e.g. ability to deal with more sophisticated forms of GVOA and support for SLA negotiation

4 Demonstrator scope and design choices

This section documents the scope of the demonstrator in terms of core functionality of the VHE and potential enhancements. It will not be possible to implement all of these enhancements during the lifetime of TrustCoM. Nevertheless it is useful to give an indication of how the demonstrator can be further developed in the future, both as a platform for future research and as a pattern for a production platform for real services. We also give an account of the rationale behind design choices made.

The first sub-section re-visits and explains the prioritisation decisions described above. Later sub-sections document design decisions for the core functionality of the demonstrator and point the way to potential extensions of this functionality. The account of the demonstrator given here is organised along architectural rather than functional lines – functional subsystems are distributed across architectural components. First the modular demonstrator architecture is described, and then the main building blocks: the integrated gateways, the central management services and other EN-wide services. The section concludes with a discussion on means of integrating with network services and other issues to do with migration to an eventual commercial service implementation.

4.1 Justification for prioritisation decisions

Previous sections have already:

- established an architecture for the demonstrator that is a specialisation of the abstract TrustCoM architecture to the VHE scenario. The main premise driving the specialisation was clear physical and logical separation of the re-usable, application-neutral functionality of the VHE from the application services and partner-specific functionality so that the former can be offered as a network-hosted service
- prioritised functional requirements in terms of necessary core functionality versus useful extensions.

The three primary aspects of core functionality identified are: Fundamental Access Control, Fundamental Monitoring and Accounting and Basic EN Membership and Service Management. Highest priority is given to **Fundamental Access Control** because:

- without a system of flexible, fine grained, context-sensitive access control that is manageable from the perspectives of individual partners and the EN and VOs the concept of agile/dynamic VO is not really viable;
- this aspect of the TrustCoM reference implementation is well-developed and embodies a number of innovations that are ripe for exploitation;
- it is potentially exploitable as a network-hosted secure resource virtualisation and exposure service even without other aspects of the VHE.

Second priority is given to **Fundamental Monitoring and Accounting** because:

- it provides the basis for a wide variety of higher-level services concerned with valuable functions such as accounting for the purposes of billing, SLA compliance monitoring, load balancing, performance monitoring, anomaly and fault detection, detection of fraud and other forms of untrustworthy behaviour;
- this aspect of the TrustCoM reference implementation is less well-developed than access control as a flexible generic capability, but has been explored in the more specific form of examples of performance monitoring in the context of SLA compliance monitoring within the two testbed scenarios;
- It is not reliant on Fundamental access control and is potentially exploitable independently of it. Note however that it is dependent on the same gateway-based infrastructure as Fundamental Access Control.

Third priority is given to **Basic EN Membership and Central Service Management** because:

- Some form of membership and service management at the EN level is necessary in conjunction with either or both of the higher priority functional sub-systems to provide support for an EN (i.e. a community of service providers) rather than to individual service providers. Note that central service management is

distinct from management of service exposure by individual partners, which is a basic function of the infrastructure and required for all aspects of VHE functionality;

- A VO Management toolkit is available as part of the reference implementation. The toolkit provides management capabilities covering the lifecycle of a 'typical' TrustCoM VO together with a graphical user interface. Some adaptation will be required to adapt the toolkit to the requirements of the AS scenario, which features an EN with many of the features of a 'classic' VO plus dynamically assembled and instantiated VOs. Some aspects of the toolkit provide more advanced functionality that required for entry-level EN support, while more basic EN management functionality is not supported. Furthermore management of the VO lifecycle in the AS scenario needs to be largely automated. It is likely that some pragmatic redesign and implementation will be required to create something simple and practical for use in the VHE context.
- It is dependent on the preceding functional sub-systems in the sense that it adds value to them by providing an extra of management functionality.

Implicitly, all three of the above are dependent on the gateway-based **EN/VO Infrastructure**, which also provides the flexibility to evolve VHE capabilities through, e.g. deployment of new and enhanced services on gateways. In a sense, then, the infrastructure has the highest priority of all. However, infrastructure is not useful in isolation, and in any case the access control functionality is already well-integrated with the infrastructure in the Reference Implementation of the Framework (in AL2). Therefore it makes sense to accord integrated infrastructure and access control the top priority, and for the combination (in conjunction with the eLearning application services) to make up the core functionality of the initial VHE demonstrator. This will then be extended with Fundamental Monitoring and Accounting and Basic EN Membership and Service Management. The result represents the minimum level of capability we expect to demonstrate by the end of the TrustCoM project. If time allows, the demonstrator will be extended with additional functionality and enhancements to the basic functionality. Note that for the purpose of WP38 it is more important to demonstrate an integrated and plausible VHE based on the TrustCoM framework rather than advanced functionality. Preference will be given to extensions that enhance the impression of the demonstrator as a rounded, usable platform for ENs.

The basic demonstrator will exercise important functionality from the following TrustCoM sub-systems:

- EN/VO infrastructure, Trust and Security Services, Policy Services – all required for the integrated infrastructure and access control
- SLA Management – lower-level aspects of SLA management to do with performance monitoring are relevant to Fundamental Monitoring and Accounting
- VO Management – required for Basic EN Membership and Service Management

There now follow a few comments on why BP Enactment and full SLA Management are seen as future enhancements to the core functionality. It is worth separating out the following aspects of SLA management to comment on them individually:

- Monitoring e.g. of performance parameters – this is included within the scope of the demonstrator, but has wider applicability than just SLA management. Note, however, that measurement of some classes of SLA-relevant performance parameter will require instrumenting of application services or the servers they run on and hence will not be possible as part of a generic, network-hosted service. In the general case, then, performance measurements provided by the VHE will be necessary, but not sufficient for SLA Management purposes.
- Monitoring of compliance with (complex) performance constraints. This is a potential future extension to the VHE monitoring functionality. Again it has wider applicability than just SLA management. Depending on the nature of the constraints, it is potentially a complex problem that has not really been studied within TrustCoM and so is not appropriate to address within the demonstrator
- Derivation of performance constraints and monitoring requirements from SLAs. Electronic representations of realistic SLAs are not yet sufficiently mature or standardised to allow implementation of generic support for them. In any case, the language of SLAs is often industry or application specific. This means that at present this aspect of SLA Management as 'part of the application'.

- Application of sanctions on SLA violation. Similar comments apply as to the previous bullets. A simple example of this has been implemented in AL2, whereby persistent SLA violation results in reduction of payments and potentially replacement within a VO. However it is a) just an example, and b) the sanctions are not derived from an electronic representation of an SLA.

We now move on to comment on to why BP Enactment was not prioritised. Here it is useful to make a distinction between:

- Use of BP-oriented representations to describe various aspects of VOs. For example, in some classes of application at least, it is quite natural to form an *ad hoc* VO by constructing or selecting an abstract business process description that would provide one or aggregated services, then selecting the partners and services that can enact the steps in the process. The structure of the VO and the description of its business processes are then closely related, and important information such as access requirements can be derived from the description regardless of whether the process description is executed as such. The VO Management, toolkit, e.g., relies on a choreography specified in WS-CDL in order to select the partners.
- Use of business process execution engines to choreograph and or orchestrate enactment of business processes. This is what is meant by BP Enactment here.

While some form of coordination of service execution is typically required within an aggregated service, it is often quite closely tied in with the application logic. There is thus a choice as to whether the co-ordination is performed by the application services themselves, or by application neutral middleware services. Which is the better option depends on the nature of the application and design philosophy adopted for the application services. Thus while BP Enactment is a useful capability for the VHE to have in case it needed within an EN, it is not needed in all ENs. Furthermore the simple form of VO typified by the eLearning application which is our design case, has a 'prime contractor' that provides an aggregating service combining input from a number of subsidiary services to produce a composite output. It is quite natural for the prime contractor's service to co-ordinate execution either integrated with its application logic or using a BP engine provided by the partner itself. The basic approach can be iterated to form tree-like hierarchy of partners and services. We feel this organisational model is fairly typical of an important class of simple ad hoc VO at which the initial VHE is aimed. Note also that BP engine is not required to co-ordinate operation of the VHE infrastructure itself as other control mechanisms are used.

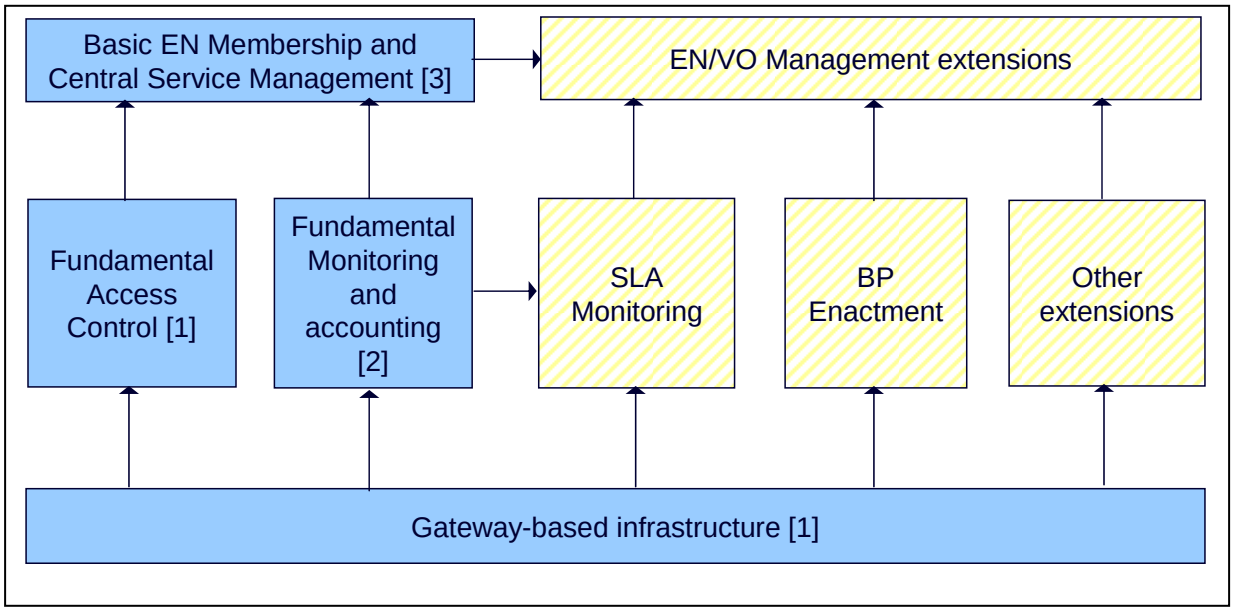

Figure 7: Core functionality and possible extensions. The arrows indicate dependencies (A is necessary for B) and the numbers indicate prioritisation.

4.2 Core infrastructure architecture

The core infrastructure for the VHE consists of a network of gateways (see Figure 2). Each gateway corresponds to a partner in the EN, and is essentially similar apart from configuration information and possibly partner- or application-specific additional or replacement services. The gateway acts as bridge between the internal world of a partner and the inter-partner world of the EN. Relative to the TrustCoM framework architecture, a gateway integrates and packages services/components that are dedicated to an individual EN partner, but are independent of the application. We may think of a gateway as being deployed on a dedicated hosted machine, and this is how the demonstrator is being implemented, but alternative options include:

- deployment of multiple gateway processes on the same host,
- deployment of gateways on virtual hosts (using e.g. VMware or User-mode Linux),
- hosting multiple virtual gateways on a web services security gateway appliance.

This modular approach has the following benefits:

- Compartmentalisation: giving each partner a dedicated (though possibly virtual) gateway benefits security by giving an EN partner unambiguous control of access to and by its own services. It also limits the vulnerability to attacks whereby someone with administrator privileges with one partner may interfere with access to services belonging to another partner.
- Scalability: In terms of core infrastructure, provisioning an additional partner consists simply of cloning and configuring a new gateway module. This means the same basic architecture can be used for all scales of EN, dimensioning the infrastructure for a new EN is straightforward, and the infrastructure can easily be expanding or contracted as partners join or leave during the life of the EN.
- Deployment flexibility: The modular approach provides for a range of deployment options. At one extreme, all gateways are located at a central facility (e.g. a server farm), at the other they are distributed around the edge of the network at local points of presence or in customer premises equipment, or actually provided and operated by EN members. Indeed, mixtures of these deployment options are possible. Furthermore, since what a given EN member ‘sees’ is its own gateway, the actual infrastructure architecture is invisible to EN members. The VHE operator can migrate from one deployment architecture to another without affecting ENs other than by changing the addresses / end point references of their gateways. This lowers market entry risk for a new VHE operator.

4.3 Gateways

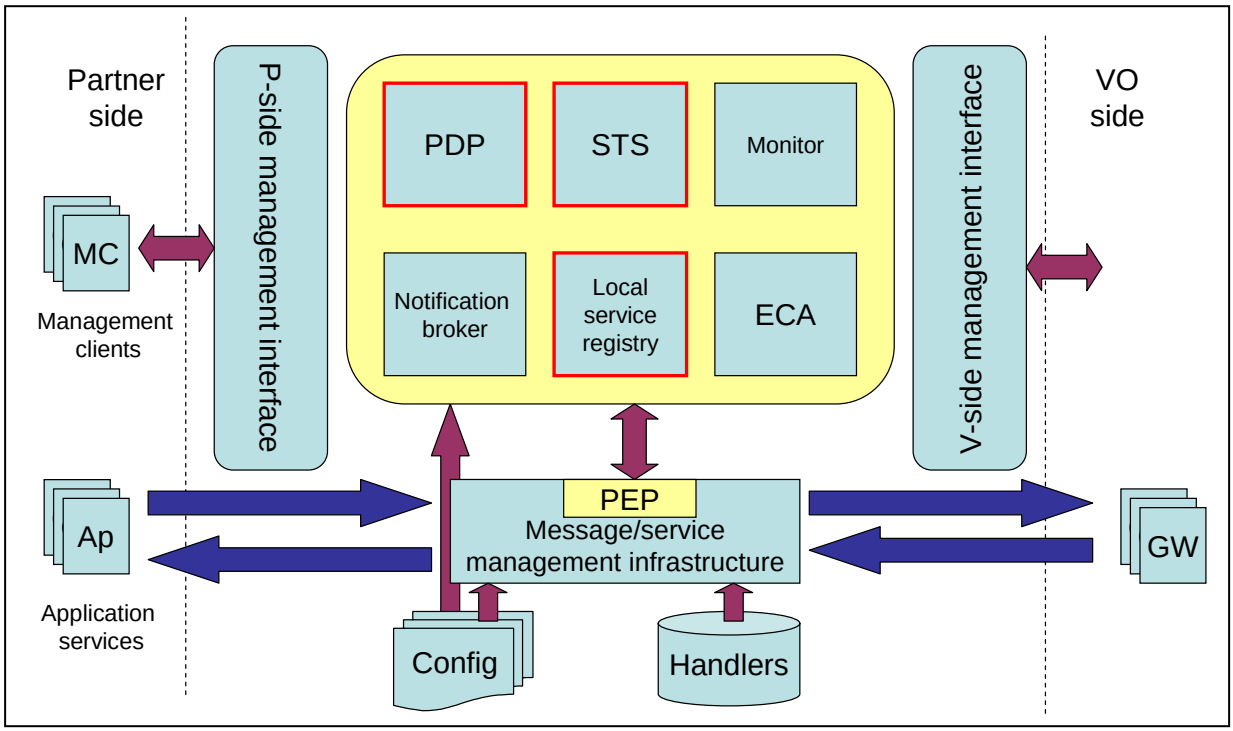

Figure 8 Gateway architecture and interfaces

The Gateway is the primary modular building block of the VHE infrastructure. It packages together a number of generic TrustCoM services on a 'per-partner' basis, as shown in Figure 8. The lower central part of the figure shows the local element of the message / service management infrastructure. Messages to and from application services of the partner are intercepted and operations are applied to them at the Policy Enforcement Points (PEP) before they are forwarded to the destination service, another gateway, or else dropped. The operations applied and their sequence depends on the message content and context as specified in configuration files. The operations are implemented mostly as modular and re-usable 'handlers', thus one way of extending the functionality of gateways is by adding to its library of handlers.

In order for a partner service to send or receive messages via its gateway, it must be 'exposed' within one or more collaboration contexts, referred to as federations. This requires instantiation of a local service identity at the gateway for each federation with which the service is exposed. These service instances:

- encapsulate the application services, controlling information about them released outside the partner enterprise including real service identity and location.
- manage state for the service in the context of individual collaborations.

Messages sent to or from application services that have no corresponding exposed service instances will be blocked at the gateway. Messages between exposed service instances will only be forwarded in the context of a federation to which both services instances belong.

Information about the service instances is held in the Local Service Registry, shown within the rounded box in the upper part of Figure 8. This box contains an extensible set of modular components used within the gateway. The components shown in the figure and described briefly below provide core functionality required for Fundamental access control and Fundament monitoring and accounting capabilities. They also exemplify how the gateway could be extended to provide additional capabilities. In most cases their functionality is invoked from the message/service management infrastructure or in response to events. An event notification is a type of message that is delivered on a 'publish-and-subscribe' basis. Notification-aware components are connected by a system of event buses. A notification producer posts notifications on an event bus when e.g.

a significant state change occurs in an entity it is monitoring; notification 'consumers[5]' listen on the bus for notifications of interest to them. The event notification service is a basic infrastructural element, complementing the service-service message infrastructure and like it is used in a variety of contexts. As well as forming part of the control mechanism of an individual gateway it can be used to coordinate between gateways and to underpin a variety of higher-level services. To preserve modularity and separate event notification traffic of different types and sensitivities, we have taken the decision to have separate event buses for intra- and inter-gateway notifications.

The highlighted elements in the rounded box in Figure 8 are directly involved in providing the fundamental access control functionality (see 3.2). The role of the Local Service Registry has already been covered. The Security Token Service (STS) is concerned with issuing, validating, exchanging, etc. tokens (i.e. credentials suitable for attaching to messages). The Policy Decision Point (PDP) makes access control authorisation decisions based on declarative policy rules. Both roles are well understood and accepted (at least at an abstract level) and governed (though not completely specified by) open standards (e.g. WS-Trust, SAML, XACML). The STS and PDP are invoked from handlers performing operations such as (STS) replacing 'internal' credentials recognised within a partner organisation for 'external' ones recognised within an EN, and (PDP) passing or dropping messages based on access entitlements.

The Event Condition Action (ECA) policy engine is used to implement aspects of gateway control functionality (including aspects of access control), but is also a useful generic building block with applicability to a wide range of services including notification and monitoring. As its name suggests it is processes declaratives rules of the form 'If an event matching template E is observed and conditions C apply, then perform action A'.

The notification broker adds value to the basic event notification mechanism. Rather than monitoring a notification bus continuously, a notification consumer may subscribe to a topic via a broker. The broker will inform all subscribers to a topic when events concerning that topic are posted.

The element labelled Monitor is representative of a class of component concerned with gathering, correlating processing, logging and/or forwarding information from 'sensors'. Typically the sensors are either implemented as handlers (collecting information derived from messages transiting the gateway) or by instrumenting elements of the VHE or application services with extensions able to generate notifications corresponding to significant events. Examples of uses to which this class of component would be put include monitoring for the purposes of logging billable events, anomaly detection, load balancing, and compliance with SLAs. We cannot implement a comprehensive range of monitoring capabilities in the time available for the demonstrator. Instead we will implement a small number of simple representative capabilities with general applicability to the monitoring of parameters concerned with simple transactions (e.g. response time, completed / incomplete transactions, etc.).

The two remaining aspects of the gateway as depicted in Figure 8 are the Partner-side (P-side) and VO-side (V-Side) management interfaces. The P-side interface provides a means for authorised administrators within the partner organisation associated with the particular gateway to control and configure the gateway. In practice, the P-side interface is a collection of web-based administrative interfaces enabling different tasks to be performed. An example task to be performed via this interface is exposure of an additional service to the EN.

The V-side interface has two aspects:

- a gateway-gateway 'control plane' interface enabling activities such as formation of federations
- a gateway-EN/VO management interface allowing agreements, policies, decisions and events at EN and/VO level to influence the behaviour of the gateways

4.3.1 Gateway implementation decisions and rationale

The baseline gateway implementation for the WP38 demonstrator is based closely on the gateway from the reference implementation in AL2. This now provides most of the gateway elements outlined above to the extent required for Foundational access control functionality and at the time of writing is approaching a state

[5] This is the term that is commonly used, but it is a misnomer, as notifications are not removed from the bus when read.

of maturity where it can be handed over to WP38. The main alternative considered was to base the WP38 gateway on a leading Commercial Off the Shelf (COTS) web service security gateway or Enterprise Service Bus (ESB) product. The advantage in a COTS-based gateway implementation is that it would be more attractive to a commercial organisation considering becoming a VHE provider for a number of reasons including: confidence in long term support and continued development, a robust and proven technical platform and the possibility of strategic relationship over a wider product range. The main disadvantage to the COTS option is uncertainty over the flexibility and extensibility of current commercial products. After due consideration it was decided that the risks in following the COTS route outweigh the benefits. However, evaluation of COTS products to examine their potential for use a basis for production implementations of the gateway will continue in parallel.

The starting point for the gateway is the corresponding component in the Reference Implementation. The main differences are the following:

- Replacement of the PDP by one based on the Delegent product from Axiomatics AB (http://www.axiomatics.com/). Axiomatics is a commercial spin-off from SICS, the partner who developed the PDP in the reference implementation. Advantages in using Delegent include support for the new XACML 3.0 standard. It is also intended for Delegent to be a commercially supported product, which adds to its credibility as part of an eventual live deployment. Delegent was not used in the reference implementation because of timing of design decisions and potential issues with open source licensing.
- Use of notification mechanism in line with standards that have matured since commitment to certain design choices in the reference implementation.
- Emphasis on the Gateway as a modular deployment unit, and hence closer integration of the gateway framework with the per-partner services that plug into it.
- Improvement of management interfaces and other enhancements aimed at creating a convincing demonstration of the VHE concept as a usable and useful network-hosted service

4.3.2 Gateway development and deployment plan

Initial version of the demonstrator (February 2007):

- Initial version of the Gateway providing access control functionality. Multiple instances of this will be deployed at BT, each corresponding to a partner in the application scenario and configured to interact with each other and the application services deployed at Atos Origin

Final version of the demonstrator (May 2007):

- Addition of notification functionality
- Addition of monitoring functionality
- Improvements to P-side management interfaces to demonstrate manageability from the perspective of individual partners
- Improvements to V-side management interface to better integrate with central EN / VO management functions
- Integration of alternative STS with ability for EN partner to chose which STS to use
- Integration of handlers to allow logging of events to audit web service and other services.

Possible post-TrustCoM enhancements:

- Migration of the gateway to a COTS appliance- or software-based platform;
- Enlargement of the library of standard handlers, especially with handlers that are easily configurable to detect message-related events on a selective basis;
- Enhancements to the monitoring functionality, including addition of more intelligent and configurable event correlation and information processing capability;
- Addition of support for BP Enactment;

- General improvements to the management interfaces and access control functionality and adaptive capability.

4.4 Central EN / VO management services

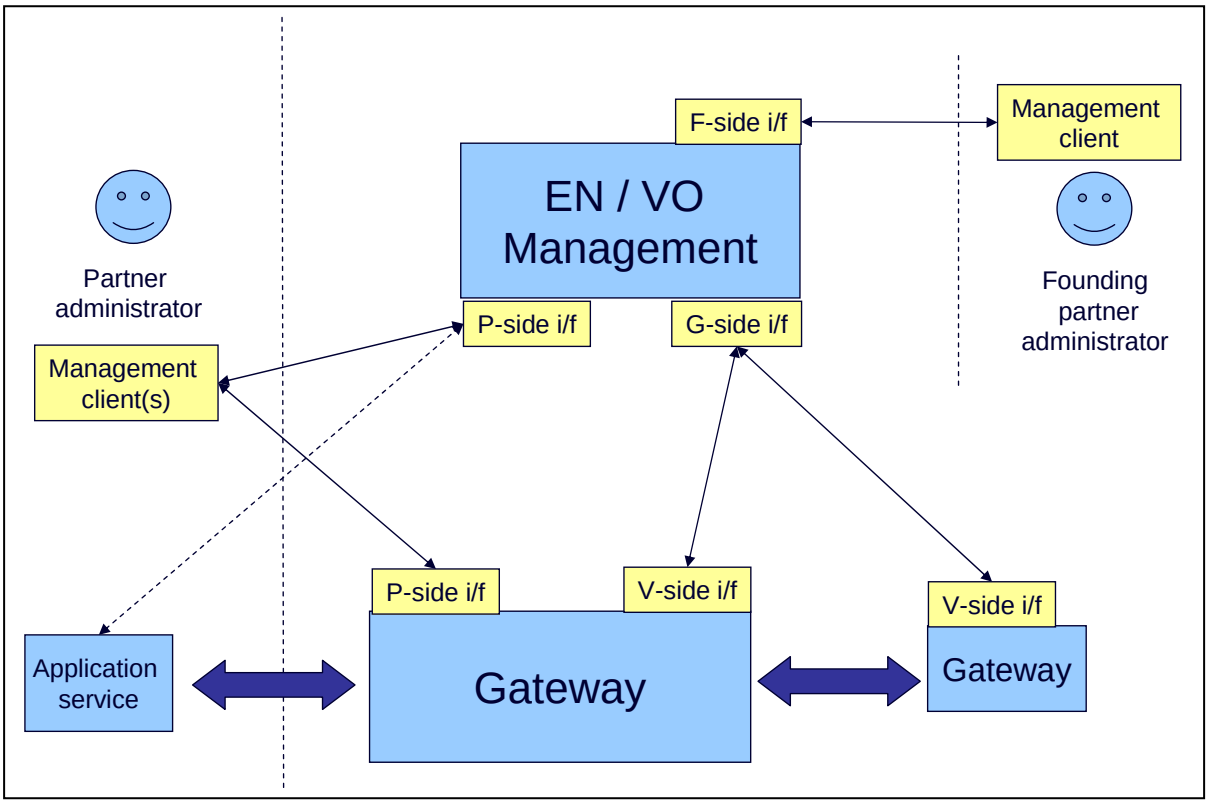

Figure 9: EN/VO management interfaces

This element of the demonstrator packages together services implementing the central aspects of EN and VO management support provided by the VHE. Recall that the overall architecture can be represented by three stacked planes: data plane, controls plane and management plane (see Figure 6). The control plane essentially consists of a federated collection of partner-specific gateways as discussed above, plus optional EN-wide services discussed below. EN/VO Management lies (primarily) in the management plane. Compared with the gateways, it deals with higher level issues concerning the EN and VOs as entities. The most fundamental of these are:

- EN Lifecycle and Membership Management: keeping track of what enterprises are members of the EN, providing means for members joining and leaving, providing means of establishing and disbanding the EN, etc.
- Central Service Management: keeping track of what services have been contributed to the EN by each partner, their characteristics, constraints on their availability, etc. The main purpose of this is to facilitate the identification of services matching desired characteristics and the formation and operation of federations and VOs.
- VO lifecycle management: Keeping track of active VOs within the EN, providing means of establishing and disbanding the EN, etc.

The above description implies the need for repositories holding information records describing: the EN, the EN member enterprises, services available with the EN, and at least the active VOs. In many cases, there are associated data structures in the control layer representing the same or related entities on a more technical level. Thus, services are represented both in the gateways and in the management plane, but the information held in the control and management plane structures is different, reflecting the different roles of the planes. Similarly, the VO (a management plane concept) is related to the control plane concept of a federation. The two are not simply representations of the same entity at different levels, however. A federation is basically an interaction context for a collection of exposed services, including policies governing permitted interactions. In the VHE, no services may interact outside the context of a federation. Consequently, a VO must be associated with at least one federation, otherwise the application services within the VO could not interact. However, in principle there may be multiple federations 'within' a VO. There may also be federations that are not associated with a VO, for example federations allowing control and management services to talk to each other. Furthermore, a federation may function as a lightweight substitute for a VO in appropriate situations.

Figure 9 shows the central EN/VO management element and its interfaces to other entities. Interaction with the:

- Founding Partner Administrator concerns EN lifecycle issues[6].
- Partner Administrator concerns a) membership issues e.g. the partner joining or leaving the EN, b) issues to do with services contributed by the partner to the EN c) issues to do with VO lifecycle management. Note that in the type of dynamic application of interest here, many interactions regarding VO lifecycle management need to be automated. In some cases it will natural for the partner side of the automated interaction to be handled by an application service. In the diagram, this is symbolised by the dashed arrow.
- Gateway primarily concerns maintaining associations and consistency between information held at the management plane and control plane levels. This includes: a) representation of services and service instances b) VOs vs. federations c) commitments to partners implied by VO membership vs. access control policies

4.4.1 Implementation decision and rationale

The primary plan for implementation this set of functions is to adapt the VO Management services from the reference implementation, namely the VO Management toolkit Host, Initiator and Member editions and the GVOA manager (which conceptually can be regarded as a constituent of the Host edition). These services deal with VOs only and not ENs, but it should be noted that the standard TrustCoM notion of VO lies somewhere between the WP38 notions of EN and VO. This is because in WP38, we are dealing with simple, often short-lived, dynamically generated VOs. Consequently the management activities (such as agreement of contracts) that need a lot of time and human involvement need to be associated with the EN rather the VO. Individual VOs in the EN, specialise and implement decisions made at the EN level. Thus, in WP38, the EN can be thought of as an abstract VO without executable business processes, while the VOs proper are lightweight entities without e.g. full-blown GVOAs. Consequently, the VO Management services are candidates for aspects of both EN and VO management in the demonstrator.

The components (editions) of the reference implementation VO Management services are as follows:

- Host Edition: this provides core services including maintenance of the information repositories and databases associated with VOs in the EN. It makes use of a UDDI repository holding EN member and service information, the GVOA manager looking after contracts corresponding to VOs, a lifecycle manager responsible for maintaining information about the state of VOs, and a membership manager that provides all functions related to participant management in a VO (e.g. adding, removing or replacing members). The host edition provides a simple, browser-based graphical user interface mostly for simple monitoring purposes.

[6] The Founding Partner is considered to be an EN member with additional duties and privileges to do with the EN as entity.

- Initiator edition: this interacts with the partner who initiates the creation of a VO and assists it in managing the lifecycle of the VO, including finding and selection of VO members/services. The initiator edition provides a comprehensive, browser-based graphical user interface tailored to the specific needs of a administrator initiating a VO.
- Member edition: this helps potential participants registering their business and services in UDDI (host edition) so they can be identified as a potential VO members by a VO initiator. It provides management functionality to enable members to confirm or reject invitations for a VO and also other performs higher-level management and configuration functions on a per-partner basis. The member edition provides a comprehensive, browser-based graphical user interface tailored to the specific needs of VO member.

Mapping these components to the VHE architecture, all the edition instances would be deployed centrally (apart client/user interface elements); one instance of the Host Edition would be required, one instance of the Member Edition for each EN member, and one instance of Initiator Edition for each EN member able to initiate the formation of aggregated services. In terms of the interactions shown in Figure 9, the Member Edition instances are responsible for interaction with gateways and interaction with Partner Administrators over service management and VO operation issues, the Initiator Edition instances are responsible for interaction with Partner Administrators over VO lifecycle issues, and the Host edition would be responsible for interacting with Founding Partner Administrator over EN membership and lifecycle issues.

At an abstract level, then, there is a good match between the requirements of the VHE Central EN/VO management function and the reference implementation VO Management Toolkit – the major functionality necessary for VO management is in place.. However, there are a number of issues requiring adaptation of the VO Management Toolkit to the requirements of the VHE. Consequently it may not be practical to achieve full integration of a VO Management Toolkit-based solution with the demonstrator within the lifetime of the TrustCoM project. The issues include

- issues of compatibility at a detailed level, between data structures and APIs at the management and control plane levels;
- sharing the standard TrustCoM VO role between the EN and lightweight VOs / aggregated services;
- providing an interface to the Host Edition to allow the Founding and other Partner Administrators to interact with it over EN membership and lifecycle issues;
- adapting the Initiator and Member Editions to support more automated VO lifecycle management.

Note that these are not fundamental problems, but rather practical issues which we may not have time to resolve fully.

Therefore, while it is intended to take advantage of the components developed and implemented for the TrustCoM reference implementation as far as possible, some contingency planning is required. Fallback options should it prove impractical to resolve some of the issue within the lifetime of the TrustCoM project involve combining pragmatic adaptation of some of the components of the toolkit with one or more of the following:

- implementation of ad hoc, application specific solutions as part of the application services;
- use of federations as light weight VO substitutes
- implementation of simplified replacements for some of the toolkit constituents. Note that some of the advanced features of the VO Management Toolkit are not required for the basic demonstrator (e.g. those to enable BP management and SLA management)

4.4.2 Development and deployment plan

Central EN/VO management services do not feature in the initial version of the demonstrator (January 2007)

Final version of the demonstrator (May 2007):

- Central EN/VO management service running at BT performing This will deal with Basic EN lifecycle management, service management and VO lifecycle management. It will work in conjunction with the ‘control plane’ mechanisms provided in the Gateways.

Possible post-TrustCoM enhancements:

- Introduction of additional management aspects of the TrustCoM Framework such as: full GVOA lifecycle management, SLA management, monitoring and enforcement and management aspects of BP Enactment
- Extension to management of functionality currently outside the TrustCoM framework, e.g. billing and revenue sharing mechanisms
- Improved treatment of contracts and SLAs, including the interface between natural language agreements and interpretations of them that can be monitored and enforced automatically.

4.5 Other EN-wide services

This section covers utility services available centrally for use in VOs formed within the EN. Typically, these will be independent of the application, but in a real VHE some services may be specialised to a particular industry sector. In the time available to TrustCoM it will only be possible to deploy a small number of basic services as examples of this class:

- Secure Audit Web Service, acting as a trusted repository to which events and documents can be sent for future reference, e.g. in case of disputes.
- Accounting log: a service accepting notification of events form which billable account information can be generated.

Arguably, the central service registry should also be included here, but it has been treated as part of the Central EN/VO Management services because of its close relation to that function.

Note that this class of services serves as a major means of expanding the functionality provided by a VHE when used in conjunction with the flexible, policy base facilities provided by the gateways. They fall into two main categories:

- those that are relatively self contained and meaningful at an application level. These can be advertised and aggregated into composite services in the same way as application services. Effectively, this means that the EN or EN host becomes a member of the corresponding VO.
- Those that contribute the central aspect of a larger block of functionality that also involves services located on the gateways and/or central management.

Note that the two categories are not disjoint, as a service of the first kind may encapsulate a more complex, decentralised service.

Examples of further functionality that could be added post TrustCoM include:

- Suitably wrapped billing and disbursement engines
- Services recording historic performance of EN members and making performance-based measures available e.g. in support of partner selection
- A recommender service allowing VO participants to submit favourable or unfavourable reports on experiences of doing business with other EN members and to obtain reputation measures based consolidated reports
- Electronic notary service
- Flexible and programmable / configurable interface onto the EN-wide distributed monitoring functionality
- Services offering monitoring and management of performance and configuration of the VHE infrastructure
- Services encapsulating capabilities offered by the underlying network. See the following section for the examples currently available via the BT Web21C Software Development Kit.
- Services offering access to wider, federated identity infrastructure.

4.6 Integration with network-based services

The VHE is envisaged as a facility that is integrated with a next-generation, converged, multi-service network (NGN) such as BT's 21st Century Network (21CN). The VHE provides a way for the NGN operator to offer higher level, added-value services to its business customers. Conversely, the VHE can make use of the NGN service-oriented capabilities (e.g. authentication, billing, etc.) as well as the ability to integrate communication services with application services, and use of the network to send web service messages.

The ability to demonstrate the potential for integration and later to trial integrated operation would enhance considerably the benefit of the demonstrator to BT. It is unlikely that time will allow demonstration of integration within the life time of TrustCoM. However, we will perform experiments to confirm the feasibility of this and investigate the best strategies for integration to allow work to continue smoothly after the end of the project and to support the credibility of the exploitation route.

Some specific issues that that are candidates for investigation are:

- trial use of heavy duty commercial off the shelf (COTS) web services security appliances as platforms for the TrustCoM Gateways. A particular commercial product has already been targeted, and arrangements for purchase of an example by BT are at late stage.
- trial use of an industry-strength COTS message bus product (e.g. Sonic ESB) such as might form the basis of future network-based SOAP message transports. This investigation would be closely linked with internal BT work on the successor to the current BT Integrate product [8].
- trial integration/interoperation with (capabilities based on) market-leading identity management and authentication products. Computer Associates' SiteMinder product is particularly import from the point of view of future exploitation within BT.
- trial integration/interoperation with a COTS billing platform
- trial integration/interoperation with one or more BT 21CN 'capabilities' (essentially service-oriented interfaces to network services)

A recent development that will make investigation of integration with the 21CN capabilities easier, is the availability of the BT Web21C Software Development Kit (SDK) Beta release [9]. Web21C is a project to make 21CN capabilities easily available to e.g. third party developers of web service applications. In Phase I, BT has already exposed a number of capabilities to developers, and a lot more functionality will be made available as time progresses. The current SDK beta release is for Visual Studio and is a set of libraries and controls for .NET that makes it simple for developers to consume Web Services exposed by BT. The Web21C SDK abstracts the services interface and serialization classes by providing the developer with a simple object model to interact with. Controls allow the developer to easily add functionality to both web and windows forms by dragging the control onto a surface and providing basic configuration options. The Web21C SDK implements features of WS-Security and WS-Trust

The following functionalities are accessible in the current version:

- Short Message Service - The Short Message Service (SMS) allows the application developer the ability for individuals to send SMS messages.
- Voice Call - The Voice Call service allows application developers to add the ability for individuals to place phone calls from their application.
- Conference Call - The Conference Call service allows the application developer the ability for individuals to place and control conference calls.
- Presence - The Presence service allows the application developer the ability to store and retrieve an individual's current status and availability for communication.
- Authentication - The Authentication service allows the application developer to create and control an authentication realm for their application. This includes management and authentication of users.
- Information About Me - The Information About Me (IAM) service allows the application developer a way to store and retrieve data about an individual in key value pairs.

- Location - The Location service allow the application developer to add the ability to determine the geographic location (latitude, longitude, altitude) of a mobile device. Currently the Location service only operates in mainland UK with BT issued mobiles, but with service providers partnering all the time, the location service will very soon increase.

All of these offer potentially useful enhancements to a variety of VHE applications including the eLearning application used in the demonstrator. If time allows, we aim to perform at least a preliminary investigation into integrating some of this functionality into the demonstrator before the end of TrustCoM.

5 Assignment of partner responsibilities

The assignment of primary responsibilities to partners within WP38 is shown in the table below

Partner	Primary responsibilities
BT	• Overall WP38 lead • Main VHE demonstrator site • Secondary partner domain demonstrator site • Integration of VHE functionality into demonstrator • Migration and further development of EN infrastructure and access control functionality • Experiments in integration/interoperability with COTS appliances, software and services and NGN capabilities
Atos Origin	• Main partner domain demonstrator site • Secondary VHE demonstrator site • Integration of eLearning application functionality into demonstrator • Migration and further development of eLearning application functionality • Joint responsibility with SICS for Monitoring and accounting. Atos will focus on the monitoring aspects.
Imperial	• Application and enhancement of ECA policy engines within the demonstrator, including application to the Monitoring and Accounting function. • Assist BT with infrastructure and access control
SAP	• EN membership and service/VO management
SICS	• Joint responsibility with Atos for Monitoring and accounting. SICS will focus on the accounting aspects. • Assist BT with aspects of access control function
UoK	• Assist BT with access control functionality, especially in respect of standards-compliant STS and PDP components. • Assist SAP with aspects of EN membership and service/VO management • Assist SICS with aspects of monitoring and accounting, especially refinement and integration of secure audit service and reputation service if this is required.

Note also that:

- some support will be available from AL2 partners in respect of reference implementation services;
- the scope for rationalisation and re-use across WP37 and WP38 will be explored. This would allow additional resources and skills to be brought to bear. An extreme case of this would be use of the VHE as the core of both demonstrators.

6 Workplan and progress to date

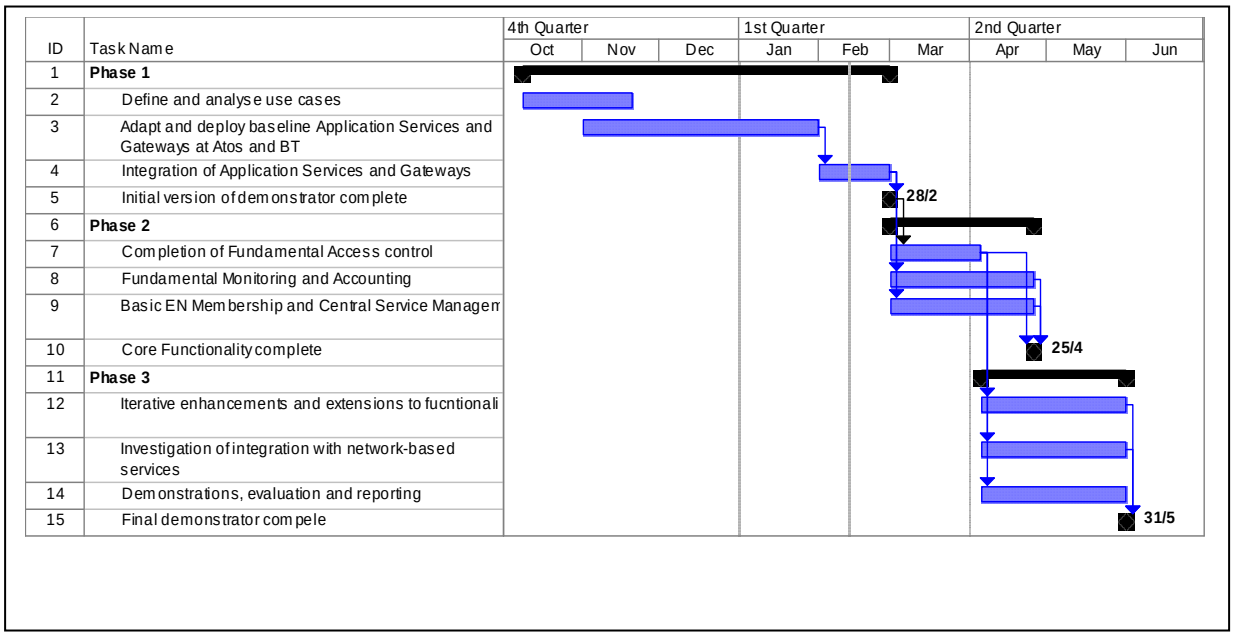

Figure 10 Work plan

Figure 10 shows the plan for the work package. Phase 1 includes definition and analysis of use cases and other preparation and planning, and production of the initial version of the demonstrator. This initial version consists of the baseline application services deployed at Atos Origin working in conjunction with gateways (one per partner) deployed at BT. The baseline gateways implement the 'control plane' elements of the access control functionality as the VHE infrastructure. The phase is relatively long because it is running in parallel with technical work in AL2 on which it is dependent and which involves the same staff. The remaining phases will proceed more quickly because more resources will be available following completion of the main technical work in AL2 (effectively marked by the 36-month project review at the beginning of March) and because Phase 1 provides the basic platform on which later work builds. At the time writing we are confident of completing the integration of the initial demonstrator before the end of February. This is one month behind target due to dependencies on AL2 and the resources shared with it. There have been no major technical problems, and the plan to use the gateway as a major architectural building block is working well.

Phase 2 will begin following the 36-month project review at the beginning of March and covers additions to the demonstrator to provide a basic level of core functionality in the three high priority areas identified and discussed in Sections 3 and 4 above: Access Control, Monitoring and Accounting, and EN Membership and Service Management. In each of these cases control plane functionality is already present to a greater or lesser degree in the gateways deployed during Phase 1, but will this be evolved and augmented at control plane and management plane levels in Phase 2. In the case of Access Control, the functionality is largely in place already and work in this phase will mainly involve upgrading the PDP, providing a choice of STS and PDP, and integrating with the other functionality as it becomes available. In the case of Monitoring and Accounting, work will focus on upgrading the Notification system and implementing example monitoring / accounting functionality. In the case of EN Membership and Service Management the focus is providing the central, management plane services and integrating them with control plane functionality in the gateways. The first choice for the central services is to adapt the VO Management Toolkit components to the requirements of this scenario.

Phase 3 overlaps somewhat with Phase 2 and will commence as at least one of the Phase 2 activities is substantially complete. Phase 3 primarily involves:

- Demonstrations to stakeholders in TrustCoM partners, the Industrial Advisory Board, and outside the project; analysis and documentation of feedback; and documentation of lessons learned during development of the demonstrator.
- Investigation of integration with network-based services as described in Section 4.6 above.
- Implementation of enhancements to the demonstrator and such additional functionality as time allows. The architecture is intended to be expandable and 'evolvable', and the functionality to be provided by the formal end of the project is limited by the available time.

Note that it is in the interests of TrustCoM commercial partners to exploit the results of the project individually and collectively. The AL3 demonstrators are an important tool in promoting the take up of the TrustCoM ideas and technology within the businesses of the partners. It is the intention of the WP38 partners to continue developing the demonstrator and using it to engage with stakeholders beyond the end of the project. Consequently the end of TrustCoM does not mean the end of the demonstrator, and in effect Phase 3 will continue for as long as the demonstrator serves a useful purpose to the partners who have contributed to it.

7 Conclusion

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

The last year or has seen the emergence of a socio-technical phenomenon that has been given the label Web2.0. According to Wikipedia, Web2.0 'refers to a perceived or proposed second generation of Web-based services—such as social networking sites, wikis, communication tools, and folksonomies—that emphasize online collaboration and sharing among users'. Technically, Web2.0 technologies are closely related to web services, but they are more user-interface focused and used to create collaborative applications that support social interaction among their users, and are often also modifiable by their users. One frequently-mentioned Web2.0 idea is the 'mashup'; basically a composite web application that can be created rapidly from pre-existing constituent services. BT and Microsoft are already co-operating on a network-based platform for mashups [10, 11]. Conceptually, the mashup is very similar to the dynamic aggregated service that the WP38 VHE is designed to support, and the popularity of Web2.0 supports our belief in the emergence of a new business model based on agile collaborations of small enterprises. The type of application envisaged for the VHE is somewhere between the current use of web services to support relatively static B2B business processes and the fun Web2.0 applications where ease of use and customisation is paramount. The VHE is aimed at the middle ground of serious business application of dynamically aggregated services in a secure and trusted environment.

This document has laid out the plan for development of a trial implementation of the VHE concept and an example Enterprise Network in the eLearning sector and reported on progress to date. The demonstrator is derived from the corresponding AS testbed in AL2 and is built largely using adapted elements of the TrustCoM reference implementation. Compared to the AL2 AS testbed the main difference is the emphasis on the VHE concept as the basis of a network-hosted service platform. There is a clean and clear separation of the application-specific services from the application-neutral core functions composing the VHE, and to enhance realism in the demonstrator the VHE and application services are hosted at different partner sites (BT and Atos Origin, respectively). The core functions are also more closely integrated to become prototype service platform rather than collection of components, and management interfaces enhanced to make the demonstrator credible for eventual business use. Some of the reference implementation elements are also being 'upgraded' to more mature equivalents that are more suited for use in live business applications. One feature of the architecture is the use of the packaged gateway (including gateway infrastructure and local 'per-partner' services such as Security Token Services and Policy Decision Points) as a modular building block. One gateway is assigned to each partner in the EN making the architecture scalable and also making a clear separation between what is under partner control and what is under control the EN or a VO.

Not all the functionality available in the TrustCoM reference implementation is included in the demonstrator as planned for completion with TrustCoM. This is because one the main design objectives was to create a well-integrated, rounded basic platform containing the essential facilities required, and to which other services could easily be added. Thus priority was given to fundamental features that are useful in wide variety of contexts (the 80-20 rule), and indeed can be built upon to create some of the 'missing' functionality. The three fundamental blocks of functionality to be implemented are Fundamental Access Control, Fundamental Monitoring and Accounting, and Basic EN Membership and Central Service Management. They are described and the choices justified in Section 4.

At the time of writing, the initial version of the demonstrator is approaching completion. It consists of the baseline application services deployed at Atos Origin working in conjunction with gateways (one per partner) deployed at BT. The baseline gateways implement the 'control plane' elements of the access control functionality as the VHE infrastructure. No major technical problems have been encountered. Progress has

been slower that originally planned but this is due to resourcing conflicts within the project, which will soon be resolved as other work packages complete.

A major purpose of the demonstrator is to engage with business stakeholders in TrustCoM partners, advisory board members and also interested parties outside the project. Such demonstrations will only become possible towards the end of Phase 2 when the core functionality will be in place, so it is not yet possible to report back on this aspect. We feel confident, however, that the demonstrator will be an effective vehicle for explaining and promoting the VHE business and technical concepts and also the overall TrustCoM Framework. Although the VHE is only one possible incarnation of the generic TrustCoM framework, it includes most of the fundamental technical features, and it is often easier to first explain a concrete instance such as the VHE and then generalise to other possible cases.

References

1. Two Scenarios for 21st Century Organizations: Shifting Networks of Small Firms or All-Encompassing "Virtual Countries"?', Laubacher et al, http://ccs.mit.edu/21c/21CWP001.html
2. 'Flexible Work Arrangements and 21st Century Worker's Guilds', Laubacher and Malone, http://ccs.mit.edu/21C/21CWP004.html
3. 'Electronically-enabled free lancing', *Harvard Business Review*, Sept-Oct 1998
4. Elance web site: http://www.elance.com/
5. guru.com web site: http://www.guru.com/)
6. hotdispatch.com web site: http://www.hotdispatch.com/.
7. D62 TrustCoM Framework V3
8. BT Integrate service information: http://www.bt.com/uk/bt_integrate/
9. Web21C SDK Developers' Centre: http://sdk.bt.com/
10. 'Microsoft and BT Launch Connected Services Sandbox Competitions' http://www.microsoft.com/presspass/press/2007/feb07/02-12SandboxCompetitionPR.mspx
11. Connected Services Sandbox: http://www.networkmashups.com/Default.aspx