Deliverable

76

Final report on legal issues

-Enforcing and monitoring of VO Contracts

WP9 Legal Issues

Dana Irina Cojocarasu,
NRCCL

13.02.2007

Version

1.0

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

Prepared for the European Commission under FP6 Contract No. 01945 as a deliverable form

LEGAL NOTICE

The following organisations are members of the Trustcom Consortium:

Atos Origin,
Council of the Central Laboratory of the Research Councils,
BAE Systems,
British Telecommunications PLC,
Universitaet Stuttgart,
SAP AktienGesellschaft Systeme Anwendungen Produkte in der Datenverarbeitung,
Swedish Institute of Computer Scence AB,
Europaeisches Microsoft Innovations Center GMBH,
Eidgenoessische Technische Hoschschule Zuerich,
Imperial College of Science Technology and Medicine,
King's College London,
Universitetet I Oslo,
Stiftelsen for industriell og Teknisk Forskning ved Norges Tekniske Hoegskole,
Universita degli studi di Milano,
The University of Salford,
International Business Machines Belgium SA .

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: 6

Activity: Analysis of Legal Issues

Work Package: 9

Task:

Document title: Final report on legal issues. Enforcing and monitoring of VO contracts

Version: 0.1

Document reference:

Official delivery date: 10 February 2007

Actual publication date: 13 February 2007

File name:

Type of document: Report

Nature: Public

Authors: Dana Irina Cojocarasu, NRCCL

Reviewers: CCLRC and Atos Origin

Approved by:

Disclaimer

This document is the result of research work carried out in the TrustCoM Project. It is not intended to be legal advice and is not to be construed or understood as legal advice. Persons interested in applying any information in this document to their specific needs are recommended to seek relevant professional legal advice regarding their specific needs/requirements.

Neither the authors of this document, nor the TrustCoM Consortium, nor the European Commission shall be liable for any use made of this document. This document does not represent the opinion of the European Community nor is the European Community responsible for any use that might be made of the content of this document.

Forum

Any dispute arising out of or in connection with this document shall be submitted to the exclusive jurisdiction of the Norwegian Courts.

Table of Content

1 Executive summary

The final Deliverable of TrustCoM WP 9, describing the research performed by the legal team during the second half of 2006 (M30-M36 of the project) wishes to carry out a comprehensive analysis of the manner in which we have achieved the research objectives envisaged at the beginning of the project and based on the lessons learn through the present collaboration, to suggest possible areas where further legal support could be provided in the deployment of legally compliant web service architectures.

In order to gain insight on the legal research that was still to be provided as input to TrustCoM, we reassessed firstly the outcomes of the research performed by the legal workpackage until present in the light of the current progress both in the TrustCoM Framework and in the two TrustCoM scenarios, aiming to emphasize the manner in which the legal requirements were reflected or integrated in the web service architecture and services developed by our project partners. Section 3.1 describes the results of this activity.

Based on this initial input, we were able to describe more systematically the legal input that we are able to provide in supporting the work done by the other TrustCoM work packages (See Section 3.2 for details).

1. By examining the TrustCoM services “active” in a certain phase of the VO lifecycle as well as the message exchanges among them, we can detect those exchanges with legal relevance (for example a negotiation, contract formation, notification, sanction) and ensure that they do fulfil the conditions typically required by law for such messages.
2. By examining the TrustCoM scenarios we are able to identify the typical business roles in the collaboration and describe their interactions in achieving a specific collaboration role. This activity sets the premises of identifying the contractual framework of the collaboration.
3. Once the legally relevant message exchanges have been identified, and the nature of the business interactions between roles has been described, we are now able to add content to those message exchanges (for example what will be the event to be notified, what will be the policy to be enforced, what will be the sanction to be taken in case of a reputation drop).
4. The rights and obligations of the business entities collaborating in a VO with a particular aim can be organised in a system of rules, which enables us to draft the contract (s) that governs the collaboration.

The three previous deliverables of the legal work package focused primarily on the third type of legal input from those described above, identifying legal requirements that should be considered when describing the behaviour of the business roles during the operation of the VO according to the two TrustCom Scenarios. In choosing this approach we temporarily prioritised the definition, selection and analysis of the legal concepts we considered to be relevant during the operation of the VO over the legal analysis of the functioning of the

Subsystems developed by TrustCoM or the contractual and policy requirements that would need to complement their deployment.

Advances in the TrustCoM framework as well as Enhanced Prototype Scenarios for both the Collaborative Engineering and the Aggregated Services Testbed allow now for a more complete legal analysis covering all the different forms of legal input presented above.

Section 4 of the present Deliverable introduces a legal perspective on the operation and functioning of the TrustCoM subsystems. The interactions among the service components in each of the VO lifecycle were examined and mapped against the typical legal events corresponding to the same lifecycle phase.

In the **Preparation phase** (Section 4.1) of the VO Lifecycle we described the legal implications of the listing by a potentially interested VO Member of a description of its business profile and of the services it is willing to offer in a Service Description Repository.

In the **Identification phase** (Section 4.2) two legally relevant events have been described: the Initiative to create a VO and the identification of EN Members to whom collaboration roles may be assigned. GVOA negotiation, regarded in the TrustCoM Framework as an event during the Identification phase, is also analysed from a legal point of view in the light of content and possible outcomes. It was also questioned how the TrustCoM Subsystems tackle frequent incidents in the formation of a contract, such as the withdrawal of the offer by the VO Initiator or the impossibility to assign validly all the Business Roles stipulated by the Collaboration Definition.

The **Formation phase** of the VO Lifecycle (Section 4.3) supports the configuration of the services participating in the VO. From a legal point of view, the SLA signing protocol has been examined and several legal requirements have been suggested for implementation.

The **Operation phase** of the VO Lifecycle (Section 4.4) is legally challenging on condition that we shift the view form the business processes to the individual participants to the VO. The two TrustCoM Scenarios were again brought into discussion, this time in order to explain the main access and obligation policies that were included in the scenario specific GVOAs provided in the Annexes to this Deliverable.

The **Evolution** of the VO is triggered in accordance with event-condition-action policies when either the membership base of the VO needs to be amended or the parameters of the service provision (such as the security settings, the business goal, or the location of the resources) need to be altered. The legal analysis of this phase of the VO lifecycle concentrated on:

I. the events leading to the modification of the membership base of the VO

II. reactive policies that lead to amendments in the access rights and authorisations during the operation of the VO

We identified legal requirements for those main events leading to the modification of the membership base of the VO, as envisaged in the TrustCoM Framework. SLA Violations, reputation drop or changing environmental conditions or customer request were discussed in this context. Their legal requirements are explained in Section 4.5 of this Deliverable.

Once the interaction among the TrustCom subsystems has been scrutinized, Section 5 and 6 of the present deliverable focused on very specific interactions that from a legal perspective condition the existence of a VO.

The first such interaction enables the **Monitoring of VO contracts (Section 5**). Where the message exchanges among the VO members are in an electronic form in order to observe in due time that a contractual breach has occurred (the notion "contract" including here the EN Agreement, GVOA, SLAs or user licenses) you need to have in place monitors that not only detect, but are also able to communicate and record in a retrievable format information that subsequently could be used as evidence. The main legal question is not how the monitors are instantiated and function but what kind of information it would be useful to monitor.

Taking as a starting point the two GVOA examples provided in the Appendixes we examined the main contractual policies and emphasized the monitoring requirements of some of them. It is to be remembered that not all the terms of a legal document can be translated at this point into objective metrics so as to automate and enforce in real time all the contractual policies. This would constitute a challenging objective in itself but it exceeds the scope of the description of work provided to TrustCoM.

Given the current state of the art in TrustCoM it was possible to emphasize elements legally relevant that can be objectified and monitored in order to support the evidentiary process but not to replace it. During the litigation, other elements will have to be taken into account as well.

On several previous occasions, discussions regarding **the enforcement of VO Policies** revealed that the legal team had a different understanding of the concept from the informatics teams in TrustCoM. A more structured and comprehensive approach of the legal view on the enforcement of VO Policies was considered to represent a useful contribution to the integration efforts made by all the TrustCoM work packages.

The final section of the Deliverable (Section 6) focused on the enforcement of VO policies on the VO Members and clarified the correlation between the legal means for policy enforcement and the technical means of implementing and enforcing policies through the TrustCoM Policy Control Subsystem. Although it is desirable that the majority of the VO Policies become enforced with as little human intervention as possible and in real time (without interrupting the system's functioning) in some instances some human involvement cannot be avoided. These circumstances were discussed in Section 6.2 of the Deliverable.

It is acknowledged that significant legal research remains to be done in the context of the service oriented architecture and we are still in an incipient phase in the identification of the challenges brought by it onto the traditional legal concepts. However, the legal research carried out as part of the 5 research strands described in the Description of Work has hopefully contributed to the creation of a legally compliant framework enabling secure collaborative business processing in on-demand created, self-managed, scalable, and highly dynamic Virtual Organisations.

2 Introduction

The objective of TrustCoM's legal work package was to study selected legal issues in relation to trust, security and contract management for virtual organisations. The work was performed by NRCCL in collaboration with SINTEF and KCL until February 2006 and by NRCCL (University of Oslo) until the end of the project.

Taking as a starting point the Collaborating Engineering testbed or the Aggregated Services Testbed, we strived to emphasize the main legal requirements that could be derived and the main challenges that might be faced from a legal point of view in deploying emerging technologies in web services such as those developed by TrustCoM. While web services allow a more flexible technical solution in discovering resources and an opportunity for businesses to collaborate in an open internet environment, they raise also questions regarding the proper access control, security, manageability or liability decisions that need to be made in order to uphold the existing legislation. If business environments are to be receptive to these applications they need to be reassured that they will not have to face unmanageable legal risks in using them.

Since the present Deliverable is the final TrustCoM deliverable to be presented by the legal team, we would like to focus firstly on the main research achievements obtained so far and their integration within the TrustCoM framework.
The first legal deliverable D15[1] introduced:

- General requirements to trust, security and contract management (in correlation with the degree of definition at that point in time of the TrustCoM Conceptual Models and Architecture).
- More specific legal issues such as private international law aspects of jurisdiction and choice of law, as well as data protection and intellectual property requirements.
- Given the collaboration with SINTEF and KCL, we introduced legal risk analysis as a novel inter-disciplinary approach for integrating of the perspectives of trust and security with the focus on legal issues related to virtual organisations.

The second legal deliverable, D17[2] focused on the legal risks in relation to access rights management, based on the ad-hoc aggregated services

[1] TrustCom Deliverable D15 " TrustCoM Report on Legal Issues", 31.07.2005

[2] TrustCom Deliverable D17, "Legal Risk Management for Virtual Organisations", 31.01.2006

(AS) test bed scenarios developed in TrustCoM. The work performed by the legal Workpackage in the second half of 2005:

- Contributed to the TrustCoM conceptual models from a legal perspective, by explaining in general terms how Enterprise Networks (ENs) and Virtual Organisations (VOs) may utilize contracts to regulate their collaboration.
- Defined a method and language for legal risk management which can be used to reduce risks related both to the technology and to the contracts in the context of the applicable statutory laws.
- Evaluated this method and language based on the experiences with the scenarios studied in TrustCoM.
- Applied the method and language to the study of access rights management issues in the context of the TrustCoM eLearning scenario. This required both a more abstract analysis of the legal basis for access rights management in the context of eLearning, and a specific analysis of legal risks related to the envisaged collaboration, which is assumed to utilize the TrustCoM technology.
- Targeted the legal risk analysis to the VO lifecycle addressed in the TrustCoM framework.

The third legal deliverable, D60 aimed at integrating the access based on policies as defined in the TrustCoM framework with the legal protection of confidential information. This report focuses only on a subset of clauses in VO contracts. Confidentiality related clauses will arguably play an important role in VO contracts in the TrustCoM context, since the collaboration of VO partners in many cases will require participants to communicate confidential information. Such information will need to be protected both though technical means – as addressed in other TrustCoM deliverables - and through the use of appropriate clauses in the contract or contracts established to operate a VO. The study:

- Provided a framework for identifying what may legitimately described as confidential information, and what action can be taken if the this type of information is improperly managed;
- Illustrated how risks arisen during or following the disclosure of confidential information can be mitigated through non-disclosure agreements
- Provided a risk checklist (Section 8 of the Appendix) that uses the legal risk analysis of the CE scenario in order exemplify risks to confidentiality in the proposed scenario as described in as described in TrustCom Deliverables D 10 and D 41 and to the business models discussed in the socio-economic analysis discussed in D 59

The current legal Deliverable wishes to attain 3 major objectives:

- To evaluate and update the main legal requirements for trust, security and contract management identified so far in the light of the current status of the TrustCoM framework and the latest developments of the CE and AS Testbed scenarios;
- To introduce a legal perspective on the operation of the TrustCoM subsystems supporting the VO lifecycle
- Ensure the integration between the different monitoring instances created as part of the TrustCom architecture (i.e at a Trusted Third party level, as well as Service Provider domain and host level) with the legal requirements of the generation of monitoring data, notification and enforcement issues;

As support in achieving these objectives, we suggest 2 possible instantiations of the GVOA (one for each application scenarios)[3]; while the legal literature provides various suggestions for contractual templates that can be tailored to various real life scenarios, we consider that by working with an instantiation of such a template we can illustrate how contracts can reflect and justify the technical decisions taken in the implementation of the TrustCoM scenarios and to better distinguish between the legal and technical means to enforce the agreements entered into by the parties.

[3] they represent Appendix A (GVOA for the TrustCoM CE Scenario) and Appendix B (GVOA for the TrustCoM AS Scenario)

3 Summary of achievements

3.1 Legal requirements in the TrustCoM Scenarios

Focusing on the two TrustCoM Testbed Scenarios, this section summarizes the legal requirements identified in the previous deliverables of the legal work package and emphasises the manner in which they were integrated in the enhanced prototypes for the Aggregated Services and the Collaborative Engineering Scenarios.

3.1.1 The AS Scenario

3.1.1.1 Description of the scenario

A detailed description of the scenario can be found in the TrustCoM deliverable D11[4]. Rather than focusing on the message exchanges between the providers of the various TrustCoM subsystems, it was considered more useful to focus on the interactions between roles during the normal operational work in the collaboration and to identify legal requirements of the scenario.

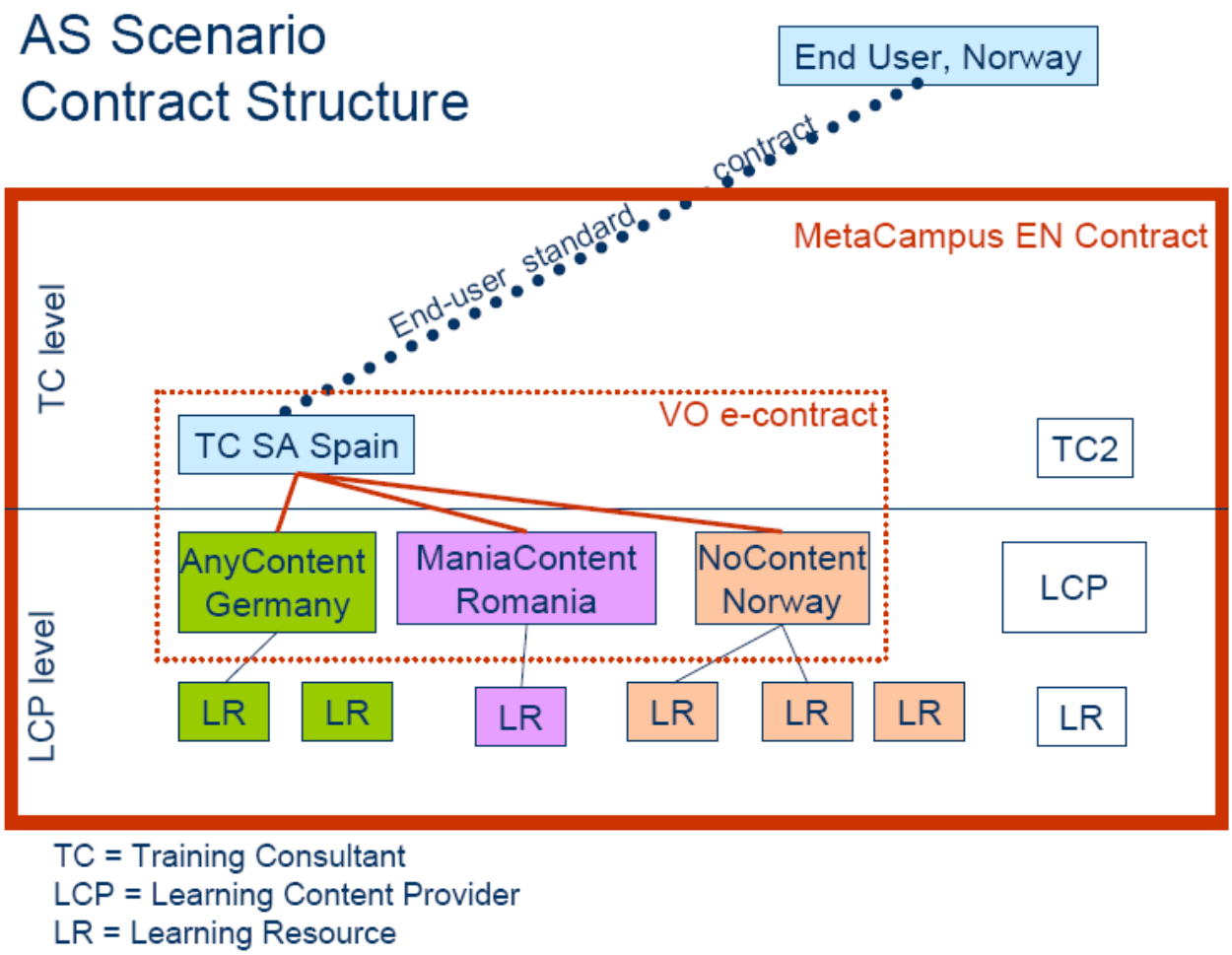
A typical business case would involve an end user interested in receiving an online course on a certain topic contacting a "VO Learning Portal Service" that is part of a "Learning Enterprise Network" and selecting a Training Consultant from those available. This might be one the user has an existing relationship with, or it might specialize in a particular topic or category of users. The Training Consultant interacts with the user to obtain training requirements, issues a User Profile, and then aggregates a Learning Path that would accomodate both the User Requirements (the previous knowledge of the user, the level of proficiency desired, etc) and the various Learning Resource Providers' availability.

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

3.1.1.2 Legal requirements

The first legal contribution to the AS scenario was the identification of its **contractual framework**. Since Virtual Organizations are not regarded as new entities with legal personality but rather instances of collaboration among VO members, a number of contracts should be put in place for the scenario to be operable:

[4] TrustCoM deliverable D11, "Baseline Prototype Infrastructure for the AS Scenario"



a. The first contract level is the **Metacampus Enterprise Network (EN) contract**, which regulates the general co-operation among the EN members. This contract will be drafted by the EN Host and adhered to by all the Learning Resource Providers (LRPs) that wish to participate in the provision of Learning Courses using the service oriented architecture of the Metacampus. In addition to the identification and contact details of all the involved parties, this agreement will contain 3 main sections: one detailing the terms and conditions for use of the Metacampus and the services available for the subscribers (that would correspond to the TrustCoM subsystems), another one describing the terms and conditions for the provision of the learning course to end users (including all the arrangements regarding the assignment and ownership of intellectual property rights and the terms and conditions of the end-user license) and a third one dealing with liability waivers and payment details for the services provided. A template for an EN contract is included in the Report Legal Issues in SME

clusters, provided by the Legal-IST project[5]. Though templates and model contracts are available, it is not possible to draft one general EN contract for all applications. There will be major differences between possible networks in various industries, services, jurisdictions, etc depending on the type of VO envisaged to be supported.

b. Secondly, once a business opportunity has arisen (i.e. an end-user is willing to execute a suggested learning path), a **General VO Agreement (GVOA)** will define how the aggregated services will be performed. A possible GVOA for the AS Scenario is provided in Appendix B of this Deliverable. In terms of the legal entities that are part of the GVOA Agreement, they are the Portal Provider and the LRPs that were selected to provide the learning resources included in a certain user's Learning Path. As a consequence, we will have as many VO's as there are learners, though the corresponding GVOAs will not be negotiated separately every time a new learner is provided the course. Rather a GVOA template will be provided as an Annex to the Metacampus Enterprise Network (EN) contract. As for the choice of making the Portal Provider a part of the VO, it is justified by the fact that it provides the services that intermediate the interaction of the LRPs with the learner throughout the entire Learning path. Therefore, no direct legal relations between the learner and the LRPs exist.
c. The third contract level will be an **end-user contract**, most likely based on a standard agreement. The end user will have to agree to its terms if he is to benefit from the learning facilities of Metacampus.

The contractual framework of the scenario has been integrated as part of the scenario storyboard and in the GVOA Agreement for the AS Scenario.

The legal analysis of the AS / e-Learning scenario focused as well on legal risks related to **international issues**, i.e. choice of law and jurisdiction. While the international nature of a VO has few implications for the computational infrastructure of a VO, it is a factor of major importance in a legal context. Most of the identified legal risks relating to international issues may be mitigated by defining an exclusive jurisdiction and an applicable national law in VO-related contracts. The remaining legal risks, particularly in relation to consumer contracts, should be tolerable and relate to the special protection for consumers[6].
The analysis is reflected in the provisions of the GVOA Agreement.

Subsequently, legal deliverable D17 identified and assessed legal risks in relation to **access rights management**. The study discussed and explained the legal rules that come into play when decisions need to be made regarding the proper design of access control technologies, the required level of protection that needs to be insured or the rights that might be claimed when circumvention occurs. Considering that according to the scenario, the decisions regarding access are taken through the automated enactment of access policies in accordance with the provisions of

[5] legal-ist.org

[6] More details relating to jurisdiction and choice of law in consumer contracts (B2C) can be found in TrustCoM Deliverable D15, Appendix B, Section 3.4.1

the GVOAs and those of the SLAs, the study underlined what the content of those policies might be and who should be the actor to approve those policies.

Decisions regarding access to Intellectual Property content are made at least in two moments in the scenario:

1. Once the LCP's consent to join the Metacampus, they should provide to Learners the agreed learning resources at any time upon specific request from the Portal Provider or from the LRP prior in the Collaboration Definition. This requirement, captured by the proposed GVOA in article 3 and 4 of Section 2 is translated in the design of the AS Scenario through the fact that the 'partner-level security token service' (STS) installed at the Portal level and at the LRP level (called STS-PP and STS-LRP) are configured in a way that they accept each other's security tokens in the scope of the Learning VO. The STS-LRP accepts security tokens from the STS-PP that contain "Learner" claims, i.e., the learning resource provider accepts statements by the portal provider that a given client is a learner[7].
2. Once the end-user chooses one of the recommended learning paths, the content which is part of the path should be made available to him in the specified order. No other content should be available to him. This requirement will be part of the End-User License, since it specifies the limits of the access rights of the user and will be found in the Access Policies deployed in the scenario.

The analysis of the access rights in the AS Scenario highlighted as well two possibilities to interpret the position of the **Portal** Provider as an intermediary in the relation User- LRP:

1. The existence of a non-exclusive **license** of the right to authorize the access to learning resources, with a conditional clause stating that the access authorization rights with regard to a certain content are transferred from the LRPs to Metacampus Prvider if that content is selected to be part of the learning path. In this case, the LRPs would not have the right to impose additional access limitations once access has been granted at the portal level (but the same content available online could be subject to different access conditions for users accessing the resources directly, outside and independent of the Metacampus framework).
2. The exclusive right to authorize the access to certain content belongs to the existing rightholder (LRP), so the access clearance takes place at LRP level. While at the Portal level the selection of authorized users takes place (through the assignment of a learning path to be followed), the conditions regarding access are set and checked by the LCPs according to their policies. The price paid for the personalized on-line course could thus reflect the different conditions imposed by different LCPs.

Since the first possibility was supported by the deployment of the scenario (see for example that the STS-LRP accepts security tokens from the STS-PP that contain

[7] see the TrustCoM Deliverable "Final Prototype AS testbed"

"Learner" claims) it was also transposed as well in the provisions of the GVOA, with the mention that this administrative assignment of the authorization right given by the LRPs (IP Rightholders) to the Portal Provider is just temporary (the license is given from the Effective Date until the user no longer needs to access that particular Learning Content).

Subsequently legal risk analysis was carried out in order to support the drafting of the GVOA clauses with reference to access rights management.

3.1.2 The CE Scenario

3.1.2.1 Description of the scenario

A description of the CE scenario can be found in TrustCoM Deliverable D 41[8].

The scenario involves a consortium of engineering companies CE VO involving a number of 'tier-1' partners who provide major sub-systems to a business jet (such as airframe, engines, avionics etc) who following negotiations with an existing customer receive the task of upgrading an aircraft fleet to support Internet access in the passenger cabin. This involves installing new antenna and communications systems into existing aircraft.

The consortium enrols a new member that has the technical expertise and the contacts required for delivering the Internet system (TC-ConsEng). During the scenario, there is an increased demand for High Performance Computing and storage facilities that are required for performing the large-scale simulations of the new antenna and communications systems. Providers of these resources (TC-HPC and TC-SP) are found and join the VO as temporary members. The service providers are intended to work together in the context of a simulation or 'job' that involves the retrieval of design model data from a provider that stores the model input data, the computation of the analysis results by the provider of HPC-based application services, and their storage on a(n alternative) provider of analysis results.

3.1.2.2 Legal requirements

The legal analysis of the CE Scenario focused only on a subset of clauses in the VO contracts. Confidentiality related clauses will arguably play an important role in VO contracts in the TrustCoM context, since the collaboration of VO partners in many cases will require participants to communicate confidential information. This information will need to be protected both though technical means – as addressed in other TrustCoM deliverables - and through the use of appropriate clauses in the contract or contracts established to operate a VO.

[8] Deliverable D 41, WP35, "Enhanced CE Test Bed", Section 5. The Document makes reference to TrustCoM Deliverable D10, "Baseline prototype infrastructure for the CE Scenario".

The study provided a framework for identifying what may legitimately be described as confidential information, and what action can be taken if the this type of information is improperly disclosed. The integration with the work performed in TrustCoM was achieved through providing input regarding the design of policies about access to confidential information as well as through suggesting appropriate contractual arrangements able to reduce the likelihood or the consequences of unwanted incidents involving confidential information[9]. The GVOA model for the CE Scenario, presented in Appendix A to this Deliverable and translated into XML format integrates the **risk checklist** provided in Appendix B of Deliverable D60 regarding the designation and protection of confidential information.

The following requirements have been given special consideration:

- A contractual clause clearly defining what information will be protected as confidential and how future information or documents deserving protection will be marked (Section 4 Article 1 of the GVOA for the CE Scenario);
- Contractual designation of circumstances in which confidentiality obligations do not exist irrespective of the content of the information exchanged (Section 4 Article 2 of the GVOA for the CE Scenario);
- Restrict access on a need to know basis and have the employees of the VO members with access rights sign confidentiality agreements (Section 4 Article 3 and 4 of the GVOA for the CE Scenario);
- Stipulate the obligation to monitor and be able to document those elements that are constituent of a crime (according to criminal law) (such as: the source of the intrusion, the exact information asset that was misappropriated, or the consequences of the intrusion) (this is the type of clause that would be found in an EN Agreement);
- Stipulate expressly in the confidentiality agreement the authorized/ non authorized uses (what is the purpose of the disclosure) (Schedule 3 of the GVOA for the CE Scenario provides a description of the Roles and implicitly of the scope of their rights and obligations with regard confidential information)
- The parties should have the obligation to return to their legitimate owner or to destroy the documents referring to the confidential information upon completion of tasks (in the CE Scenario, the confidential information of one VO Member, such as its preexisting technology does not leave the domain of that partner. What is being granted and revoked are authorizations to access them)
- Insert a clause of “agreed payment for non performance”. Thus, the rightful holder of information will be entitled to claim from the receiver the agreed sum of money whatever the extent of the actual prejudice he suffered (Section 4 Article 6 of the GVOA for the CE Scenario).

[9] See TrustCoM Deliverable D60, ”Report on Confidentiality Clauses in VO Contracts”

In addition, section 4.5 of Appendix A of TrustCoM deliverable D60 discussed the **advantages and the shortcomings of the business models for the CE Scenario**[10] in what concerns the protection of confidential information.

- Where CE VO maintains direct contractual relationships with all other involved actors (TC-HPC, TC-SP, TC-ConsEng), which thus are directly bound to the conditions agreed with the CE VO. This model implies arguably the highest coordination costs for the CE VO, but on the other side it affords maximum control. The disadvantages of this business model regarding the management of confidential information are:
    - It creates for it a need to enter into confidentiality agreements with each of these suppliers and monitor in each case the manner in which the contractual obligations assumed by the partners are respected.
    - Since the nature of the business relation is different with regard to each of the suppliers (a consultancy contract with TC-ConsEng, a service provision contract with TC-SP and another one with TC-HPC), the nature of the confidential information exchanged and more importantly, the specified purposes allowed under the confidentiality agreement differ. Moreover, since these partners handle (access and use) confidential information at different moments in time, the duration of their obligations differs as well. That makes it highly unlikely that one single standard-form and all inclusive confidentiality agreement could be envisaged for all of these business relations.
- In a classical sub-contracting model, the CE VO subcontracts with the consultancy company Cons-Eng, which again establishes and maintains contracts with TC-HPC and TC-SP. This model transfers some of the management and coordination to TC-ConsEng, but may contribute to a reduction in control of the subcontractors. The amount of control will essentially also depend upon the constraints imposed on TC-ConsEng with respect to subcontracting, e.g. whether TC-ConsEng may freely choose subcontractors, whether the subcontracting organizations and their employees will be subject to specific non-disclosure agreements, etc .In this case,
    - It is possible for CE-VO and TC-ConsEng to agree on certain confidentiality policies involving all confidential information to be exchanged throughout the collaboration, regardless the identity of the involved VO members at a certain point in the collaboration. TC-ConsEng will have the possibility to impose this standard on the second tier suppliers as a precondition for collaboration.
    - However, in case the second-tier suppliers do not respect the compulsory standards of confidentiality or the imposed access procedures, the CE-VO will be able to enforce the contract only

[10] The business models for the CE scenario, are analyzed in more detail in the TrustCoM Deliverable D59, “Business Models, supplier scoring and reputation”

against the TC-ConsEng, a solution that may in practice prove slow and with limited use

- In case collaboration between TC-ConsEng, TC-SP and TC HPC is established, these partners will together have contractual relations with the CE VO. The level of control may to a certain degree depend on whether the collaboration between the three organizations is of a mere contractual type, or whether a new business entity with legal personality is established. This model:
    - facilitates a more all-inclusive model if confidentiality agreement, especially in terms of those common provisions that are likely to appear in such an agreement (for example the information that is to be designated as confidential, the symbols that are supposed to make it identifiable as such, the duration of protection, the procedures involved in the destruction or the return of the documents once the tasks are completed).

3.1.3 Legal requirements common for the AS and CE scenarios

In addition to the scenario specific requirements, the legal work package identified a series of legal requirements that are common for both scenarios. They were introduced in TrustCoM deliverable D15 and relate to the data protection requirements needed to be in place in order for a reputation system, used to evaluate the reputation subject's conduct and make this evaluation accessible for other users' decisions:

• Participation in a reputation system should be limited to actors who have expressed their well-informed consent.

• The purpose(s) of the reputation system should be clearly defined.

• The collection, storage and dissemination of (personal) data should be limited to the amount necessary to achieve the purpose(s).

• The procedures regarding the collection and evaluation of personal data should be transparent and communicated in a comprehensible way.

• Reputation subjects should be allowed some participation and control with respect to the collection of data about them and with regard to the generation of their reputation profile.

• The quality of both the collected data and of the aggregated reputation profile should be valid with respect to what they are intended to describe and relevant and not incomplete with respect to the specified purpose(s).

• Fully automated decisions on the basis of reputation profiles should be avoided. If they are chosen, there should be full transparency regarding the algorithms used to calculate the reputation score and to make the decision.

Additionally, the data subject should be able to claim a human decision.

• The security of (personal) data must be ensured.

• Reputation systems that deal with sensitive data should use a stricter policy to protect personal data.

Those requirements are implemented in the TrustCom reputation systems and partially in the provisions of the GVOAs for both scenarios.

3.2 Methodological approach for the current legal research

The main idea underlying the involvement of the legal work package up until this point was that the service oriented architecture developed by TrustCoM needs to be not only technically viable but also legally compliant. The most proactive manner to achieve compliance with the law would be to identify relevant legal requirements and to support their integration in the technological solution provided. In this case, it is the law that constrains the adoption in a concrete case of one technological solution over another or the specification of certain guarantees during implementation.

On the other hand, in ensuring that the designated beneficiaries of the TrustCom technology are being given the possibility to find out about the legal consequences derived from the deployment and use of the TrustCoM web-services, it is the configuration of the technology that dictates what legal terms and conditions should be agreed by the parties and what legal consequences can be derived from them. The contractual arrangements will in this case have to reflect and uphold the system architecture.

As explained in detail in section II.1.b of the Framework Deliverable V4 (D63), TrustCoM is developing a set of functionalities provided as services or components and grouped into subsystems, that would support (in a service oriented architecture) the realisation of dynamic virtual organisations in a secure and contract managed environment. Those subsystems are, in accordance with the Framework, VO Management, Business Process (BP) Enactment and Orchestration, SLA Management, Trust & Security Services, Policy Control and EN/VO Infrastructure. As illustrated by the two TrustCom Scenarios (CE and AS), each modularised service or component is activated in a certain manner in order to support the events that occur during the phases of the VO lifecycle.

The design of the TrustCoM subsystems themselves allows for limited contribution from the legal work package. Our involvement becomes however more relevant once those components are being interconnected in order to support the VO lifecycle, as this interaction should illustrate how business entities using the TrustCom technology assume certain roles in a collaboration that functions in accordance with the law and the business practice.

Based on the experience accumulated so far in the TrustCoM project, we are able to describe more systematically our approach in providing legal input supporting the work done by the other TrustCoM work packages. In order to explain the rights (permission, prohibitions) and the obligations of the VO Members (in our case of the Roles) in specific collaborations that rely on service oriented architecture (such as the TrustCoM AS or the CE Scenarios) we need to:

1. ***Identify the TrustCoM services "active" in a certain phase of the VO lifecycle as well as the message exchanges among them***. The legal input in this case would consist in making sure that a message exchange with legal

relevance (for example a negotiation, contract formation, notification, sanction) fulfils the constraints typically required by law in terms of, for example:

a. Entities that have to be aware of that message exchange;

b. Entities that have to approve/ agree on the content of the message;

c. Data that has to be stored as proof of that message exchange;

d. Consequences of that message exchange (subsequent events that are triggered by that exchange).

2. ***Identify by looking into specific Collaboration Definitions the ROLES that can later on be assigned to an entity with legal personality (natural or legal person).*** If the previous step raised research issues related mainly to general legal concepts, this step (as well as the following two) is to be seen strictly in connection with a certain collaboration scenario. Since the law can assign rights and obligations only to legal entities and not to services or other software components[11], the legal input that can be provided in this step consists in the identification - based on a suggested Collaboration Definition[12] - of the various tasks that businesses are supposed to fulfil and their position in the overall collaboration. This would include also identifying legally compliant policies to manage the situations in which the identity of the businesses fulfilling a defined role, changes (corresponding to the Evolution phase of the VO lifecycle).

3. ***Describing the interaction between ROLES, that is identifying the rights and the obligations associated with the fulfilment of certain ROLE.*** The legal input in this phase would consist in assessing the behaviour of the roles in each of the phases of the VO Lifecycle. Once the legally relevant message exchanges have been identified in the first step, and the nature of the business interactions between roles has been described, we are now able to add content to those message exchanges (for example what will be the event to be notified, what will be the policy to be enforced, what will be the sanction to be taken in case of a reputation drop). This content will constitute in fact the specification of determined rights and obligations of the business entities collaborating in a VO with a particular aim.

4. ***Organising the rights and obligations in a system of rules, that is drafting the contract (s) that governs the collaboration (GVOAs in particular)***.

The three previous deliverables of the legal work package focused primarily on the third stage from those described above, identifying legal requirements that should be considered when describing the behaviour of the business roles during the operation of the VO according to the two TrustCom Scenarios. In choosing this approach we temporarily prioritised the definition, selection and analysis of the legal concepts we considered to be relevant during the operation of the VO over the legal analysis of the functioning of the Subsystems

[11] the issue of autonomous electronic agents is outside the scope of this discussion

[12] see WP2/21

developed by TrustCoM or the contractual and policy requirements that would need to complement their deployment. The nature and scope of a legal research do explain this choice.

Essentially, laws (as well as contracts) describe permitted interactions between various entities with legal personality (be it companies, partnerships, individuals) as well as consequences for non-compliance. As such, in order to depict and define “the rules of the game”, we require relatively detailed descriptions of the interactions between the subsystems developed by TrustCom as well as descriptions of the business processes that those subsystems would support in both the Aggregated Services and Collaborative Engineering Scenarios.

Advances in the TrustCoM framework as well as Enhanced Prototype Scenarios for both the Collaborative Engineering and the Aggregated Services Testbed allow now for such a complete legal analysis, which follows the 4 steps mentioned above. The legal requirements identified in the previous legal deliverables will be reassessed in the light of these new developments in the subsystem design in order to illustrate more clearly their conceptual and functional integration with the work performed within other TrustCoM work packages.

4 A legal perspective on the operation of the TrustCoM subsystems

In accordance with the Methodology presented in Section 3.1 this Section will proceed to the analysis of message exchanges among the TrustCoM subsystems in order to depict those data exchanges with legal relevance (for example a negotiation, contract formation, notification, sanction). It will be assessed whether or not those exchanges fulfil the logical steps and the legal requirements that have to be met by those legally relevant events. Where it is appropriate, alternative interactions will be suggested. In addition, the legal implications of those legally relevant message exchanges will be pointed out.

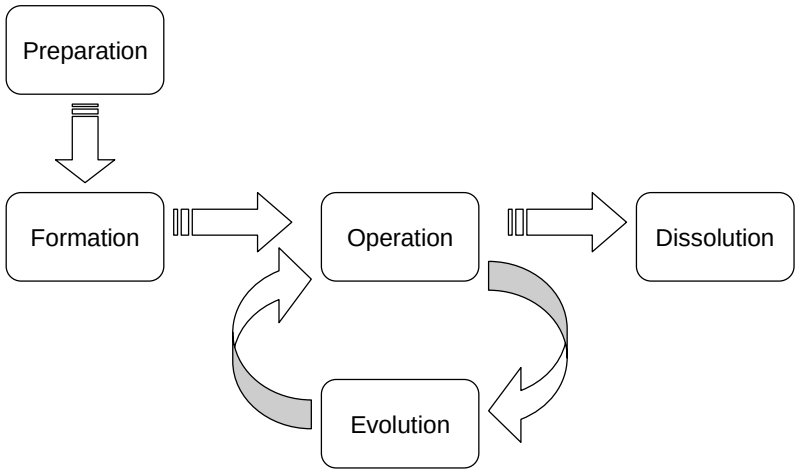
Before examining each of the lifecycle phases in the existence of a virtual organisation it is important to make one preliminary observation:

We should distinguish between the TrustCoM subsystems components and the legal entities that provide those components (are legally responsible for their functioning). Due to the nature of the Service Oriented Architecture, it may be envisaged that each service component is provided by a different legal entity. As a consequence a multitude of mini-license or collaboration agreements would be entered into before providing them in an aggregate fashion to potential service consumers. However, conceptually speaking such a scenario would bring little contribution to the research objectives aimed at through the present research project. They can be much easily (however just as thoroughly) explained by assuming that one legal entity is providing (or has been licensed) one TrustCoM subsystem.

From the perspective of the businesses potentially interested in using the TrustCoM technology in order to set up a VO or become a member of one VO, the identity of the initial rightholder for the various TrustCoM subsystems would bear little relevance. Although the subsystems and their components could be exploited separately, if they are to be interrelated and used throughout the entire VO Lifecycle (as an integrated support solution for businesses setting up a VO), it is very likely that they will all be part of a Marketplace, Metacampus or Enterprise Network,. The Marketplace will acquire (non exclusive license) all the rights in the technology before providing it to the potentially interested parties. That does not mean that the location of the components change, the architecture will still be distributed, however, in the relation with potentially interested VO members, there will be only one legally responsible partner representing the other service providers in that particular context.

This assignment of rights would arguably occur as part of an ***Enterprise Network Agreement*** that would specify in addition to the identity of the initial rightholders in the various system components also the terms and conditions of use of the platform by its subscribers (potential VO members). Throughout this deliverable, other possible contractual clauses of the EN Agreement will be identified.

In the lifecycle of a Virtual Organisation, the following phases have been identified:



4.1 The Preparation phase (pre-VO)

The preparatory phase in the formation of a Virtual Organisation is the creation of a pool of organisations willing to join virtual organisations. To that extent, the interested organisations will register to an Enterprise Network which will list the organisations and the services they are willing to provide.

From a technical standpoint, registration of a potential VO Member will involve its listing of a description of its business profile and of the services it is willing to offer in a Service Description Repository[13]. TrustCoM does not bind this service description to formalism meaningful for an automatic discovery. However it anticipates that these descriptions have associated SLA Templates that are stored in a SLA Template Repository[14]. Upon subscription, the SLA Templates are filled in with meaningful information regarding the ranges for Quality of Service parameters that the provider is willing to accept as starting point in negotiations. References to a SLA Signer service that will perform the signing of a concluded agreement on behalf of the service provider are also provided.

From a legal point of view, by subscribing to the Enterprise Network they become involved in two different legal relations:

1. In relation to the Enterprise Network Provider, the potential VO member manifests its consent to be bound to the terms and conditions for the use of the Network, that is agrees to the **Enterprise Network Agreement**. This will most

[13] See Section III.1.a of the TrustCoM Deliverable D63, *"The TrustCoM Framework V4"*

[14] See Section III.2.a of Appendix B of the TrustCoM Deliverable D63, *"The TrustCoM Framework V4"*

likely be a standard terms agreement, through which the Enterprise Network Provider informs it about:

a. the services and subsystems that are available for him to use upon membership in a VO and the TSC conditions for their use;

b. the obligations it has towards the infrastructure and other service providers;

c. other issues: delegation and assignment of administrative authorities, explanations about the technical steps that lead to the conclusion of legally binding agreements between members…

2. In relation to other potential VO members (at this stage just EN members or maximum VO Initiators), by joining the EN and registering its User Profile in the Service Description Repository it makes **an invitation to treat,** that is manifests its willingness to provide services to a VO within the qualitative parameters specified in its SLA. That invitation to treat is not yet an offer therefore does not create an obligation to reserve or make available resources, and it is not necessary to include details regarding the manner in which the service will be provided or the remuneration for the service provided. Moreover, that invitation to treat can be modified unilaterally at any point. All registered members can be said to have made this invitation to treat upon registration.

4.2 The Identification phase of the VO lifecycle

The identification phase of the VO lifecycle is initiated upon the manifested wish of an EN member to find business partners with which to collaborate in achieving a certain goal. In technical terms[15], this is done through the successive invocation of different services. The VO Initiator notifies the VO Management Service about the intention to create a VO. In order to reach the collaboration goal, the VO Initiator makes use of either a Collaboration Definition Repository provided by the EN, or of its own repository[16], so as to describe in a work-flow like choreography how this goal is to be achieved. Based on the collaboration definition, **roles** will be identified and those roles will be assigned to **suitable business partners.** Those potential partners will be sent invitations to join the VO. Assuming they agree to join the VO, they will be considered VO members and the Formation Phase of the VO Lifecycle can be initiated. If they don't agree, other potential VO partners can be invited for negotiation.

As it results from the technical description, the main events occurring in the Identification phase are:

a. An initiative to create a VO coming from one of the registered members of the Enterprise Network

[15] See Sections III.1.b and VI.2.c of the TrustCoM Deliverable D63, *"The TrustCoM Framework V4"*

[16] See TrustCoM Deliverable D63, *"The TrustCoM Framework V4"* page 63

b. The description of the work-flow like choreography on how the collaboration goal is to be achieved (including the business roles and the support services required and the order in which they are expected to interact)

c. The identification of EN members to whom the roles may be assigned.

From a legal point of view we are especially interested in the first and the third event from those described above.

Firstly, the manifested initiative to create a VO would create obligations for both the VO Initiator and the VO Host[17].

By communicating its intention to form a VO, the VO initiator manifests an explicit intention to be part of a VO, which is one element of a valid offer[18]. By specifying exactly the terms on which he is to collaborate, the goal of the collaboration and the resources needed (through specifying the Collaboration Definition and the Public Business Process involved), the original invitation to treat is converted from a legal standpoint into **an offer** to collaborate in a certain VO, addressed to yet unidentified contractual partners. The partners are however identifiable, based on the criteria specified in the Collaboration Definition (CD). At this point the VO initiator should specify for how long the offer remains valid. During the validity period, the terms of the offer cannot be modified.

At the same time, the VO Host will have to reserve and to activate for the benefit of the VO Initiator the resources/services it agreed to make available to the EN subscriber via the EN Agreement. The Initiator should be able to benefit (should have available), for example, the CD Modeller (component for defining the collaborative business process)[19] , CD Repository, BP Parts Modeller (so as to be able to extract Business Roles from the CD), the Discovery Service (in order to identify which of the registered members of the EN can fulfil the Business Roles). In the EN Agreement, we may specify an Entry Date (the date when a business joined the VO) and an Effective Date from which the above mentioned obligations become active. In this manner we can ensure the efficient allocation of the resources (services, components) on the Enterprise Network.

The offer should be specific enough so that in theory a simple acceptance from a business partner to lead to the conclusion of the collaboration agreement. However, due to the practical complexity of making compatible and interconnecting services located in different domains it is likely that a separate, technical document will complement the offer from the VO initiator, and its terms will have to be agreed prior to the formation of any legal understanding between the parties. This technical document is the Service Level Agreement (**SLA)**.

---

[17] The VO Host is considered here to be the business entity legally responsible for the functioning of the Metacampus/ Enterprise Network/ Marketplace.

[18] "A proposal for concluding a contract constitutes an offer if it is sufficiently definite and indicates the intention of the offeror to be bound in case of acceptance" (article 2.1.2 UNIDROIT Principles of European Commercial Contracts (2004)).

[19] See TrustCoM Deliverable D63, *"The TrustCoM Framework V4"* page 94

The specification of the Collaboration Definition, the derivation of the Business Processes and the identification of the Business Roles that can contribute to the achievement of the VO goal are essentially technical steps, with little or no legal bearing [20] on the valid formation of a VO. What is worth pointing out however is that if a service made available by a provider other than the VO Initiator is used in the assignment of business roles or in identifying potential EN subscribers able to fulfil a role this **assignment of an administrative authority** will have to be explicitly provided in the EN Agreement. The rules of mandate will most likely be applicable in this case[21].

The third event with legal relevance is the identification of the EN members to whom the collaboration roles will be assigned. Those possible partners will receive a copy of the CD and will be responsible for deriving from the "global model"[22] their own Private Business Processes and in accordance, decide whether to join the envisaged VO or not. This aspect will be captured by the GVOA through a clause allowing the VO members the freedom to decide in which technical manner they are to fulfil the obligations associated with the role assigned.

The following are legal prerequisites in the identification of possible VO members:

a. The selection of qualified partners should be fair and non-discriminatory. The criteria used in the selection should ensure a high profile of the participants, however should not exclude the newcomers on the market.

b. The VO Host is to be waived from any liability regarding the actual capacity/ availability/ expertise of the selected potential VO partners to perform the obligations associated with a Role. The parties themselves will be responsible for the fulfilment of their contractual obligations. It is true that a rating/reputation system will be used to determine the trustworthiness of the EN Members, and the EN should be expected to use the best efforts in order to create accurate criteria to be included into the Business Card of that partner[23] (stored in the common repository and used by the Discovery Service). However, it is the EN members themselves that feed in the information about their capabilities and the services they are willing to provide and this subjective determination cannot be imputed to the VO Host.

The identified potential VO Members will be sent invitations to join the collaboration. This invitation should contain at least 2 elements:

a. A proposal of a Service Level Agreement, containing information about the parties' identities (the VO Initiator as the offeror and the proposed partner)

[20] Unless we consider the liability of each individual TrustCoM subsystem service provider in case the malfunctioning of one of those subsystems.

[21] Where the mandatary is the provider of the service used for the identification of possible business partners on behalf of the mandator.

[22] Framework Deliverable V4, page 94

[23] idem, page 102

the location of the service agreed upon, the definition of monitors and metrics used to quantify the service, the QoS parameters[24]

b. The collaboration definition as proposed by the VO Initiator – this will describe the goal of the collaboration, the role to be assumed by the proposed partner as well as legal policies, which would later on constitute the basis for the GVOA.

This scission between the operative and the management terms of the collaboration would prove useful especially in the Evolution stage of the VO Lifecycle, when some service providers will decide either to join or to leave the collaboration, situation calling for their replacement. While a new SLA will be negotiated in order to integrate that Private Business Parameters of that new provider into the ongoing Public Processes of the VO, the management policies will just have to be adhered to, without a prerequisite for negotiation.

In addition, while the legal policies constituting the main part of the future GVOA are designed to be included in a multi-party agreement to be entered into by all the VO members, the SLAs regulate the service provision monitors and metrics agreed to between a service provider and a service consumer. Therefore, the SLA terms (including the TTP that they may use) will have to be agreed firstly by the provider and the consumer of the service and subsequently the results of their negotiation will be made available to the rest of the VO partners. There will be only one GVOA per VO, incorporating as many SLAs as there are Roles.

Negotiation is regarded in the TrustCoM Framework as part of the Identification Phase since it may lead to the need to identify new partners to replace the ones that declined the offer to join the VO. Additionally it may lead to modifications in the collaboration definition (through outsourcing, inclusion of additional TTP services) or in the parameters included in the proposed SLA as the concrete circumstances regarding the collaboration with the chosen service provider come into play.

In the current state of the TrustCoM framework negotiation is handled by the VO Manager and restricted to a single round of offer-acceptance[25]. Moreover, negotiation involves only the SLA, with no reference to the other non-operational aspects of the collaboration that would normally appear in a legal document. According to the TrustCoM framework deliverable, “the intelligence required to negotiate an agreement would be in the hands of a human operator or some external module that will be consulted by this component (the SLA negotiator).

From a legal point of view, negotiation that leads to the formation of the VO needs to be more closely analysed, especially since human processes will be relied upon in addition to the automated ones.

The first question to be answered is what would be negotiated at this point.

If the VO Members are to collaborate in a Service Oriented Architecture, operative SLAs parameters should be agreed first.

[24] idem, page 98

[25] idem page 100

As opposed to the situation of the EN Agreement, where the subscribers just adhere to standard terms and conditions imposed by the EN provider, the parties joining forces on a specific project need to agree afterwards on detailed obligation and access control policies and clearly define key concepts that are used within the policies. These will be gathered under the term of **General VO Agreement (GVOA)**. In case a conflict between partners arises, this agreement will be regarded as "the law of the parties" and the policies describing the required behaviour of the parties as well as expected sanctions will be used in determining liabilities for contractual breaches. It is therefore vital for the parties to decide how to, for example, define and manage the access to confidential information, manage situations in which third parties become involved and are assigned rights in the Project or the situations in which the achievement of the collaboration goal becomes impossible. Appendix A and B of the present deliverable illustrate possible terms and conditions of the GVOAs entered into by the VO members in the TrustCoM CE and AS testbed scenarios.

The simplest scenario would be that the negotiation leads to the assignment of all the roles in the Collaboration Definition (that is, the suggested EN members accepted to join the collaboration) so that the VO can be formed and become operational.

It is possible however, that following the negotiation some of the roles in the Collaboration Definition have been validly assigned, while others have not. This situation is only partially explored by TrustCoM and its management would most likely be entrusted to human negotiators. However, TrustCoM might be required to support the operation of the VO in any of those hypotheses. Based on a legal risk assessment of the concrete requirements of the Collaboration Goal, one of the following solutions may be chosen by the negotiators:

1. If the role not assigned is required at a later stage in the collaboration definition, then the parties may agree to initiate the business processes that they can handle at that point while requiring from the VO management to examine again the UDDI repository for other suitable partners. Alternatively, the parties themselves may find a suitable Partner, who may or may not want to join the EN but still wish to participate in the VO. It is unclear how the TrustCom subsystems will deal with the collaboration of a party which is not subscriber to the EN.

2. One potential VO Partner may choose to make a partial acceptance, conditioned (suspensive condition) on the valid assignment of the other roles in the project within a certain time interval[26]. That partner will not be considered a member of the VO at the point of the conditional acceptance. However the commitment to join the project would give right to the VO Initiator to obtain some damages for bad faith behaviour in case the partner refuses to

[26] "Where in the course of negotiations one of the parties insists that the contract is not concluded until there is agreement on specific matters or in a particular form, no contract is concluded before agreement is reached on those matters or in that form" (article 2.1.13, UNIDROIT Principles of European Commercial Contracts (2004)) .

join once the condition is fulfilled[27]. As a consequence for TrustCoM, the Identification phase of the VO Lifecycle and the message exchanges among the appropriate subsystem components will continue either until all the roles are assigned, or until it becomes certain that they cannot be assigned in due time, therefore creating the need for an alternative Collaboration Definition in which the roles would be more easily manned.

3. Faced with the impossibility to assign some of those roles (that is to obtain the acceptance from the partners that were potentially assigned those roles), the remaining VO Members (willing and available to join the collaboration) may decide to take over some of the responsibilities of the role unassigned so that the VO becomes operational. This business option, supported by human decisions may interfere with the configuration of the TrustCom services. It is at this point unclear how TrustCoM would address the situation where the Collaboration Definition is modified -through a human decision- in what concerns the scope of the roles assigned. Would the VO members be able to determine the reconfiguration of the interactions among the TrustCoM subsystems so as to support the new public business processes?

As part of the Initiation phase is worth analysing one more incident that can hinder the valid formation of the GVOA. That incident refers to the decision of the VO Initiator to withdraw or to revoke the offer it made. As explained above, the VO Initiator made an offer by specifying the Collaboration Definition. Based on that offer, the VO host (Enterprise Network Provider) will activate the Membership Management who will invoke the Discovery tool and start identifying potential VO Partners. This offer will become active the moment it reaches the offeree, that is when it is communicated (and becomes accessible) to a potential VO Member. Currently TrustCom does not provide an implementation of the technical steps to be followed in order to implement/ take act of the Initiator's decision to withdraw the offer. It should be possible for the VO Initiator to communicate its decision to withdraw or to revoke the offer made and to stop all the processes involved in the initiation and the formation phases of the VO lifecycle.

Moreover, if the VO Initiator is not also the Client of the VO, the other VO Members may wish to collaborate regardless of the offer withdrawal. One of them should take over the Initiator Role while maintaining the same Collaboration Definition. It is unclear whether this occurrence would be supported by TrustCoM.

As to the legal consequences of the offer withdrawal (that can of course be expressed as event –condition –action policies in the EN Agreement[28]), the law distinguishes the various moments or circumstances when the withdrawal/ revocation may arise. Article 2.1.4 of the UNIDROIT Principles of European Commercial Contracts (2004) reads:

---

[27] "It is bad faith, in particular, for a party to enter into or continue negotiations when intending not to reach an agreement with the other party" (article 2.1.15 (3) UNIDROIT Principles of European Commercial Contracts (2004).

[28] Such policies will most likely be part of the EN Agreement and not in a GVOA since this event occurs prior to the formation of any VO, hence prior to the generation of a GVOA.

"(1) Until a contract is concluded an offer may be revoked if the revocation reaches the offeree before it has dispatched an acceptance.

(2) However, an offer cannot be revoked:

(a) if it indicates, whether by stating a fixed time for acceptance or otherwise, that it is irrevocable; or

(b) if it was reasonable for the offeree to rely on the offer as being irrevocable and the offeree has acted in reliance on the offer.

In situation (1) there will be no sanction for the VO Initiator towards the EN member selected by the VO Manager as suitable to fulfil a collaboration role since no contract was concluded among them. However, since the VO Host used or reserved resources and services in trying to find suitable VO Members, its provider may seek to recuperate its costs and be thus entitled to damages. Of course, this bad faith behaviour will also probably lead to a decrease in the reputation score of the Initiator.

In situations 2(a) and (b) the VO Initiator will owe damages for the loss caused to all the parties that relied on the offer being active throughout the stated time interval.

From a legal point of view it is difficult to draw a clear line between the Identification Phase and the Formation Phase of the VO Lifecycle, especially when considering the contract negotiation to be part of the identification phase (as envisaged in TrustCoM).

The VO contract (the GVOA Agreement including also the agreed SLAs) is considered to be concluded and legally binding on the parties as soon as they agree to be bound to it. A notification of acceptance communicated to the offeror would in most cases[29] be sufficient for the contract to be considered as concluded, hence legally binding on the parties. Other formalities could be stipulated in order to ease the evidentiary process, but they do not condition its validity[30]. The notification of acceptance is regarded however in TrustCoM as the final moment in the Identification phase and not the moment where the GVOA is formed, because indeed at this point the identity of the VO Members is known.

For the purpose of integrating the legal research with the work performed in other TrustCoM work packages, we may consider that the EN Agreement stipulates another step to be made in order for the agreement (GVOA) between parties to be considered legally binding: the parties should "sign the agreement in the presence of a notary" who will keep a record of the signed agreement for further reference.

4.3 The Formation phase of the VO lifecycle

Once the identity of the VO Members fulfilling the Collaboration Roles is known, the services participating in the VO will need to be configured so as to support the

[29] the solemn contracts would be an exception, but they are beyond the scope of this deliverable.

[30] See article 2.1.1 of the UNIDROIT Principles of European Commercial Contracts (2004): "A contract may be concluded either by the acceptance of an offer or by conduct of the parties that is sufficient to show agreement".

monitoring[31], the distributed enactment[32] of the Collaboration Definition and of the VO policies as well as secure communications between VO Members. The service configuration involves[33] *"(1) the configuration of the provided service (respectively the infrastructure) itself, e.g. so as to meet the agreed QoS, or to actually deploy the necessary services etc., and (2) the configuration of the components related to the underlying (TrustCoM) framework, e.g. providing the monitor with information what services to supervise how, deploying the policies*".

Already at the end of the initiation phase the GVOA comprising all the SLAs agreed by the parties and the legal terms and conditions that define the "rules of the game" within that specific VO have been determined. Using the TrustCoM AS and the CE testbed scenarios as examples of collaboration goals, two possible project-specific GVOAs have been provided in the Appendixes to this Deliverable.

As part of the formation phase, VO Manager initiates an SLA signing protocol[34]. According to the Framework Deliverable, the signing protocol involves a Notary that first collects all signatures, verifies them and then distributes the signed contracts among the signatories. The Notary communicates the result of the negotiation to the VO Manager, and stores the signed contract in the SLA Repository. If the EN Agreement subjects the valid formation of the GVOA to the parties' signing the contract in the presence of a Notary, then some legal requirements should be considered:

1. the parties themselves are required to sign the GVOA, in a manner that certifies the identity of the signatory party, the integrity of the document signed and the non repudiability of the document (that is the party cannot deny having signed the agreement). In other words, the notary cannot collect the signatures of the parties beforehand, sign the agreements and distribute the signed copies to the VO Members. The Notary will:
    a. Collect the signed GVOAs from the parties.
    b. Verify (possible by using that parties' public key- which is part of that party's Business Card) the party's identity and the integrity of the GVOA
    c. Store the signed GVOA's for further reference (audit or enforcement purposes),
    d. Notify the VO Manager that the GVOA is now in force and the VO can start operating.
2. the VO Members may sign the GVOA at the moment of the acceptance of the VO Initiator's offer (if the acceptance is unconditional) or after being notified that all the Collaboration Roles have been manned (if the acceptance was conditional of the successful allocation of all the Roles);

[31] Monitoring of the GVOA will be addressed in Chapter 5 of this Deliverable

[32] Contract enforcement will be addressed in Chapter 6 of this Deliverable

[33] see Framework Deliverable V4, page 52

[34] see Framework Deliverable V4, page 100

3. for evidentiary purposes, the VO Members should receive proof that all the other VO members have validly signed the GVOA.

4.4 The Operation phase of the VO lifecycle

During the Operation Phase, the VO partners collaborate in accordance with the Collaboration Description in order to achieve the Business Goal. It is the Lifecycle phase where, through successive invocations of the individual application services data sets are processed and policies are enacted.

Two conceptual comments need to be reminded here.

The first one is that the web service based message exchanges between Business Roles may be front ends to complicated tasks involving human beings and all types of resources. Those Role specific tasks are to be executed in accordance with the access control policies and the obligation policies stipulated by the GVOA. In addition, "*although it would be desirable to automate the transformation of GVOA terms and conditions into policies that can be enforced by the system this is not feasible in the general case. Partial automation techniques for policy refinement in VO environments were not within the scope of the TrustCoM project and remain an item which will require further investigation at the end of the project*."[35]

The second conceptual comment worth reminding refers to the distinction between the VO's view on the business process and the view on the individual participants: *"whilst the former focus on the message exchange between the service providers, but does not provide any details regarding the actual execution of the individual roles, the latter describes the details per role and intermediate interaction partners, but does (in itself) not allow insight into the overall process*"[36]

Since the operation phase is to a large extent goal oriented, a more relevant legal input would be provided by emphasising at this point the VO's view of the individual participants rather the VO's view on the business processes (as it is the case for the other VO Lifecycle phases). I will therefore analyse the two testbed scenarios and explain the legal interactions between business roles as they are reflected in the GVOA provided for each scenario[37]

4.4.1 The Collaborative Engineering Scenario

As described in Chapter 3.1.2, the legal analysis of the CE Scenario was until now focused on the analysis of the contractual arrangements that need to be put in

[35] See Framework Deliverable, page 108

[36] See Framework Deliverable, page 54

[37] see Appendix A for the CE testbed scenario and Appendix B for the AS Scenario

place by the parties in order to ensure the proper management of the confidential resources disclosed as part of the collaboration.

At this point, through suggesting a General VO Agreement we aimed at providing a comprehensive legal framework of the collaboration, which integrates the legal view with:

- The TrustCoM high level architecture as illustrated in the "Enhanced CE Testbed"[38], especially regarding the objectives and the requirements of the testbed.
- The TrustCoM business models[39], especially the VO Business Structure of the CE Scenario

The General VO Agreement for the CE Scenario includes all the rules agreed among the parties to govern the collaborative business processes. In a relatively stable and long lasting VO, such as that envisaged by the scenario, in which the high value information assets exchanged or made available by the partners are protected by Intellectual Property Rights, VO Members would definitely be interested in retaining a high degree of control on the policies that are expected to uphold. Thorough negotiations are therefore expected both regarding the SLA parameters and the legal terms and conditions in the GVOA. Appendix A presents, only for exemplificative purposes, a possible result of these negotiations.

In addition to stating the identity of the contractual partners, defining the key terms that are to be used in the agreement and the goal of the collaboration, the most extensive part of the GVOA describes the policies that govern the relations among the VO parties as well as those among the VO Parties and third parties.

4.4.1.1 VO Parties Policies

This section will list and explain authorization and the obligation policies[40] that are enacted in the interaction between VO Parties during the Operational Stage of the Collaborative Engineering VO Lifecycle:

- In case the Party's reputation score drops at the level 0.5, that Party's will be considered as "unreliable" and thus the message exchanges which are intrinsic to its fulfillment of the assumed Project Role will be recorded and stored as evidence for future dispute resolution. The party will be under audit until an increase in the reputation role (Section 2 article 3 (a))
- In case the Party's reputation drops at level 0, that Party will be expelled from the VO.(Section 2 article 3 (a))

These two event-condition-action rules are formulated in accordance with the current implementation of the reputation system, where values 1, 0.5, 0 reputation values are described. Since as mentioned before, this collaboration is a rather stable and long lasting (as opposed to for example one aiming at the delivery of an

[38] TrustCoM Deliverable D41 "Enhanced CE Testbed".

[39] TrustCoM Deliverable D59 "Business Models, Supplier Scoring and reputation".

[40] In accordance with the dichotomy in Section V of the Framework Deliverable, Appendix B

e-learning course to one single user), the replacement of a VO member is a rather exceptional occurrence, determined either by the manifested wish of a partner to leave the VO or a significant breach in the obligations assumed.

- Neither Party shall, disclose, use or make available to its employees, advisers, consultants or third parties any confidential information of any of the VO Parties other than to the extent necessary for the purposes of the Project or the exploitation of any Project Technology;
- Every Party shall take such steps as may be necessary to ensure the safe custody of any Materials relevant to any Pre-existing Technology or Project Technology and any document containing or recording the same which is in its possession or control and to restrict access to them to the extent necessary to comply with those provisions.
- VO Party disclosing confidential information shall take all reasonable steps to ensure (including but not limited to entering into confidentiality agreements where appropriate) that the receiving entity keeps the same confidential and does not use the same except for the purposes for which the disclosure is made
- The confidentiality policies (Section 4 in the GVOA) have been extensively explained in TrustCoM legal deliverable D60 to which reference should be made.
- During the Project each Party shall ensure full disclosure to the other of all Project Technology (Section 5 article 2)
- All Project Technology and all Intellectual Property in respect thereof shall belong to all the Parties
- Other access policies are included in Section 6 article 1 and 6 of the GVOA for the CE Scenario.
- If any Party or Parties obtain in any country Intellectual Property protection pursuant to Section 7 Article (2) (b), the other Parties shall have no rights under that Intellectual Property in that country, unless such other Parties reimburse and share equally … the costs which were incurred in obtaining and maintaining the same, and to share equally the future costs of obtaining and maintaining the same.(Section 7 Article 3)
- A Party must notify in term of 3 days any inability to perform its obligations due to force majeure, and such notice must state all the particulars of the force majeure. Notice in term of 3 days must also be given by such Party when the force majeure ends. If the delay due to force majeure continues for more than 7 days the party may be expelled (Section 8 Article 4(b)).
- Event condition action policies leading to the expulsion of a VO Party can be found in Section 14 Article 3 of the GVOA.

4.4.1.2 VO Party- Third Party Policies

- The Parties will not directly or indirectly solicit, initiate or engage in negotiations or discussions with any third party regarding the object of the

Project unless and to the extent justified by the fulfilment of the role assumed through the Agreement.

This policy permits the Parties to choose themselves the means through which they will fulfill the roles assumed.

- Access policies involving third parties are included in Articles 4 - 6 of Section 6 of the GVOA for the CE Scenario
- Where a Party has compensated the third party who made a claim against the VO, such Party may exercise a right of recourse against the Responsible Party or against all the other Parties for all damages awarded, costs, expenses and charges (including legal fees) it paid (Section 9 Article(6))

4.4.2 The Aggregated Services Scenario

The TrustCoM AS scenario is essentially different from the CE Scenario, despite the fact that the underlying technology and the message exchanges among participants are configured in a similar manner. The AS Scenario envisages a multitude of short term collaborations for the provision of tailored e-learning courses to individual users. There are only two distinctive roles in the collaboration, Portal Provider and Learning Resource Provider, which simplifies the contractual framework and contributes to its standardization among the different collaborations. Although the provision of each learning course involves the creation of a new VO (involving always the Portal Provider and the Learning resource Providers selected to be part of the Learning Path), the GVOA for those VOs will not be negotiated with each new end-user, but rather instantiated based on a template Annexed to the Enterprise Network Agreement[41].

In addition, the client of the VO is in the AS Scenario (as opposed to the CE Scenario) external to the VO. The learner is not regarded as a VO member due to the fact that there is no direct legal relation between him and the Learning Resource Providers, but rather all access rights are cleared through the Portal.

Some of the standard access and obligation policies[42] in the AS Scenario are:

- Learning Resource Providers have the duty to reserve the Learning Resources agreed to be part of the Learning Path from the Effective Date and to ensure the availability of those Learning Resources at any time and for as long as the user would in normal circumstances need them to acquire the envisaged knowledge or skills. (Section 2 Article 3)

This policy is meant to ensure the optimization of the resource allocation for the Learning Resource Providers. Although some of their resources are part of the provision of the Learning Path, there is no requirement to have them available

[41] the elements that are instantiated in every VO are marked in red in the GVOA model for the AS Scenario (Appendix B to this Deliverable)

[42] reference should be made for details to the GVOA for the TrustCoM AS Scenario, Appendix B to this Deliverable

before they are actually needed. In this context, as a reflection of the fact that the Application Service Providers themselves are responsible for the instantiation of the Collaboration Definition, one LRP (Learning Resource Provider) will have to notify the following one when the user is being examined based on the part of the course already completed. The date of the notification is the Effective Date for the provider being notified.

In this manner we also take into consideration the subjective elements of the course provision, where it cannot be anticipated beforehand the speed with which the learner will go through the learning material (with enough certainty so as to set deadlines).

- In case the subsequent Learning Resource in the Learning Path becomes or is envisaged as being unavailable at the Effective Date, its Learning Resource Provider will have to notify the Portal Provider (so as a replacement can be found in due time)
- Regarding the reputation related policies, since in the AS Scenario the timely availability of the learning resources is of the essence, a new policy has been added in addition to those already mentioned in the CE Scenario: the possibility for direct elimination of the LRP who delayed the provision of the agreed resource for longer than 20 min.
- The Training Consultant Service Provider is solely entitled and responsible for the designation of the Authorized User. The Learning Content Providers shall refrain from hindering the access through legal or technical means to a Learning Resource designated as part of that Authorized User's Learning Path (Section 3 Article 2). This policy will have a corresponding one in the End-User Licence, explaining to the end – user that the authorisation received for the access to the various learning resources that are part of the learning path are temporary and sequential.
- The Learning Resource Providers grant for the License Period to the Metacampus Portal Operator a non-exclusive, non-transferable right to access the Learning Resources, use technological measures that enable the Authorized User to search, view, display and download the Learning Resources on the Authorized User's terminal.
- The Learning Resource Provider reserves the right to withdraw from the Licensed Material any Learning Resource that is part of the Learning Path, upon a minimum of 3 days prior notification to the Metacampus Portal Provider
- The Learning Resources are provided on an "as such" basis, and the Learning Resource Provider does not give any express or implied warranty towards the end user that Learning Resource will be suitable for any particular requirement, is complete, accurate or up to date. (Section 6 article 7). However, although the LRPs will not have an obligation to keep the learning material complete and up to date, failure to do so will reflect on that provider's reputation and will probably decrease its chances to be selected again in a new VO.

4.5 The Evolution phase of the VO lifecycle

This phase is triggered in accordance with event-condition-action policies when either the membership base of the VO needs to be amended or the parameters of the service provision (such as the security settings, the business goal, the location of the resources) need to be altered. Although such events occur during the Operation of the VO, they may lead to partial repetition of the Identification-Formation phase and therefore they are treated separately in the Framework.

From a legal perspective, it is relevant to analyse:

I. the events leading to the modification of the membership base of the VO

II. sanctionatory policies that lead to amendments in the access rights and authorisations during the operation of the VO

According to the framework, the VO membership base can be modified as a reaction to:

a. a SLA Violation[43].

b. a reputation drop

c. changing environmental conditions/ customer request

a) In this case, a notification from the SLA Evaluator or from the Policy Enforcement Point to the Policy Decision Point signals the discrepancy between the SLA agreed quality of service parameters and the actual parameters of the service provided. Such notification is matched to an existent policy so that actions can be executed. If the dispatch of a VO Member represents the reactive action to be taken, this action is modelled in the TrustCoM architecture similarly with the Dissolution of the VO, only restricted to that VO Member. That is, "*all active business processes of the according service(s) are stopped and all security tokens and policies that implicitly define the access rights of the respective service are destroyed – revocation of such access rights here means that all participants in the virtual organisation are instructed not to accept the respective tokens any more. Furthermore, the SLA contracts with that respective service(s) come to an end and all SLA management related services are stopped, since the monitored data is no longer valid and would cause unjustified violation messages*." [44]

The legal requirement of notifying the Service Provider prior to its dispatch is however acknowledged[45] in the Framework. In addition, it should be possible for the dispatched Service Provider to receive evidentiary support in arguing its case during litigation.

Although what is technically referred to in the TrustCoM framework as Evolution represents a part of contractual enforcement and will be further addressed in Chapter 6, some additional legal requirements could be mentioned at this point.

---

[43] See the Framework Deliverable page 56

[44] idem, page 60

[45] idem, page 59

1. First of all it is worth discussing the notification obligation. As a default rule[46], the party has to be notified that in accordance with the terms of the GVOA it is being despatched from the VO. In case that VO member provides more than one service within the VO (as it may be the case where it fulfils more than one collaboration role or just one, but very complex) it should be made clear whether the dispatch concerns only one service provided or the entire role (s) assumed. In addition reference should be provided to the SLA provision/ GVOA clause that was violated and to the location of the logs regarding the violation.

2. The revocation of all the security tokens and the access authorisations of the VO Member dispatched should not prevent the provider from obtaining in due time the evidence needed in order to contest the decision of the VO. That means that he should still be able to access all the logs that were made regarding his activity in the VO up to that point and to be able to make copies from it (and submit them as evidence in court).

3. The dispatch decision may also include a term in which the party may contest the automatic decision and a possibility for the conflict to be solved amiably without the recourse to a court of law. In simple cases, exchange of logs or monitoring data between the provider to be dispatched and the VO Manager may lead to the clarification of the cause in real time and in an automatic fashion (as it would be the case where an error occurred).

b) it is acknowledged by TrustCoM that the reputation information contributes to ensuring secure and trusted interactions among the service providers. Due to the parallel involvement of the same service provider in more VO's it is possible that their performance in different VO will feed back on their reputation[47].

In the current implementation, the reputation of a Vo Member is imported into the VO from an external reputation system at the start of the VO and exported back to the external system when either the VO is dissolved or the partner is dispatched. It is questionable for how long it is viable to consider those performance records as reflecting the trustworthiness of a VO Partner. If say due to temporary circumstances a partner's reputation drops from 0.5 to 0[48] and as a consequence it gets dispatched from that VO, it will have no possibility to be selected in a new VO since the Membership Manager verifies among other the Reputation of the service provider when identifying potential VO partners for a new VO. If there's no possibility to participate in a new VO and perform well, there will be little or no chance to "clean its record" (regardless of external, offline data confirming otherwise)[49] . The only possibility for that VO member to be included again in a VO would be to offer the only service available on the EN at a certain point, and its availability to weight more then the reputation of the provider.

---

[46] see article 7.3.2 of the UNIDROIT Principles of European Commercial Contracts (2004)

[47] see the Framework Deliverable, page 56

[48] idem, page 105

[49] see also the section indicating how the update in the reputation score of a VO Member can occur

A more advanced system would enable keeping more updated records of the VO Members' performance through the periodical synchronization with the external reputation system. In this case, a drop in reputation in a VO would become available to the other VOs in which that Party is providing the same service, likely generating changes in the access rights or the tokens of that provider (for example, this provider will start being subjected to monitoring for audit purposes). The fact that the Reputation Evaluator would convert the specific performance data (confidential information) into standard reputation information maintained by the Reputation Manager outside the VO would in this case be a disadvantage, since it would provide no information regarding the causes of the reputation drop in the first place. We could therefore question to what extent a sanction taken in a VO (the drop in reputation is a sanction following faulty behaviour of that party) can legitimately be extrapolated to another VO, especially since the context of the service provision will differ and each VO will be governed by different GVOAs, therefore react differently to the same events (see for example the TrustCoM testbed scenarios, where the delay in access to a certain resource may lead to a minor reputation drop in the CE scenario and to the dispatch of the provider in the AS scenario).

c) Virtual Organisations are created in order to cover a potentially temporary market niche. Therefore, changes in the environment (e.g. market niche being sufficiently covered by other enterprises) may lead to externally triggered evolution of the VO. Since only the parties of an Agreement can (and have an interest in) amending it in order to address better the challenges encountered in practice, an externally agreed decision (offline, such as in the case of the negotiation) will have to be communicated to the VO Manager and/or the VO Host. In this case, the VO members that are disadvantaged by this reorganisation may require damages for all the expenses incurred thus far with the organisation and deployment of the Business Processes.

4.6 The Dissolution phase of the VO lifecycle

To a large extent, the Dissolution of the VO equals the concomitant dispatch of all the VO members. Therefore, the comments expressed as part of the Evolution phase remain valid in this phase also, at least in cases where the dissolution of the VO is a sanction and the Goal of the Collaboration has not been reached (unsuccessful collaboration).

Where the Collaboration Goal has been reached, payment for the services provided will be claimed by all the participants. While TrustCoM does not provide new means for financial audit, it is possible for the VO Members to rely on their own such services and use the SLA Management capabilities of TrustCoM[50].

In addition where new Intellectual Property Assets were created as part of the collaboration, the partners will get involved in negotiating their assignment.

[50] see Framework Deliverable, page 61

The information designated as confidential during the Collaboration and disclosed among the VO Members will remain confidential for the entire period specified in the GVOA (that is, after the dissolution of the VO). It would be useful that the message exchanges involving confidential information during the Operation of the VO be always monitored and logged. In order to facilitate the evidentiary process in case a conflict arises, VO members should obtain evidence during the Dissolution phase as to the information they designated as confidential, the identity of the partner to whom it was disclosed, the moment of disclosure and the purpose for which the disclosure was made. In addition, the other VO Members' commitment to safeguard the confidentiality of the information disclosed to them is registered in the GVOA. The fact that the Notary Service will no longer be accessible to the parties after the Dissolution phase of the VO does not hinder the evidence process, since in the Initiation phase, each VO Member received from the Notary copies of the GVOAs signed by the other VO Members.

5 Monitoring of VO contracts

5.1 The configuration and role of monitors in the TrustCoM framework

In the TrustCoM framework, the monitor and the evaluator components are being configured as part of the Formation phase of the VO Lifecycle.

In the TrustCoM framework, the monitor and the evaluator components are being configured by the VO manager as part of the Formation phase of the VO Lifecycle. Two types of monitors have been configured:

- Internal monitors- they have direct access rights to the resources they inspect
- External or TTP Monitors, who lie outside the control of the service owner and can only inspect web services at their interfaces;

The main role of the monitors is to supervise the execution of a service, host process or even business process, and compute SLA parameters according to the metrics defined in the agreed SLAs[51].

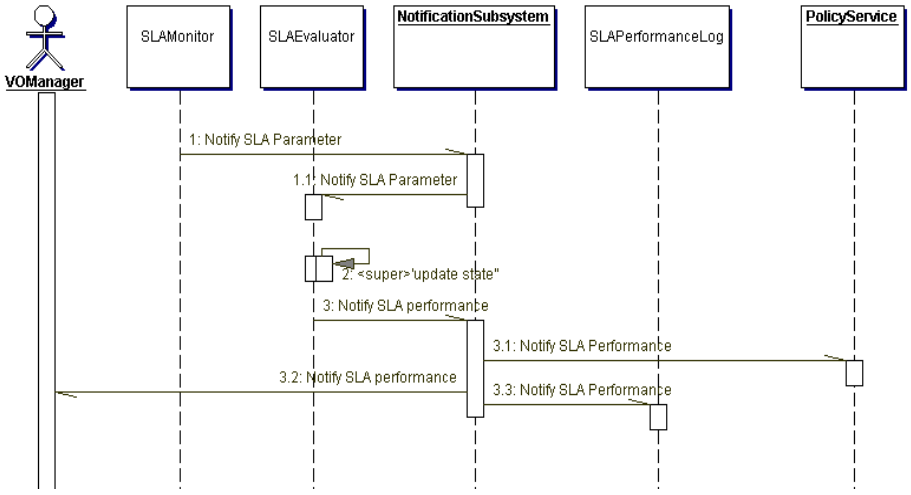


Figure 1 SLA Monitoring (according to the TrustCoM Framework)

As emphasised in Figure 1, the Monitor sends notifications to an Evaluator who, at its turn, will send notifications in the event of SLA violation and/or fulfilment to the VO Management and/or Policy Services. The processes that are subject to QoS requirements will be constantly monitored during their enactment. The current status of the monitored service will be communicated to the policy and reputation related services, thus reflecting on the reliability of the service provider.

[51] see TrustCoM Deliverable D63, *"The TrustCoM Framework V4",* section III.2.e

Monitoring the performance of the processes that are part of the Collaboration Definition as well as the quality of the services provided in accordance with the SLAs, is considered to be an essential element in order to ensure transparency for the behaviour of the software and of the organisation operating through it as well as the predictability of the ability of that organisation to fulfil a certain role in a VO.

5.2 A legal perspective on monitoring

While monitoring is seen in the TrustCoM framework as an element in Trust Management enabling predictions about the future behaviour of a service provider, from a contractual perspective monitoring appears as a prerequisite for contract enforcement. According to Black's Law Dictionary, "enforcement" designates the "act of putting something into effect". In our case, what need to be put into effect are the agreed terms and conditions for the provision of services in a VO.

Where the message exchanges among the VO members are in an electronic form in order to observe in due time that a contractual breach has occurred (the notion "contract" including here the EN Agreement, GVOA, SLAs or user licenses) you need to have in place monitors that not only detect, but are also able to communicate and record in a retrievable format information that subsequently could be used as evidence.

The main legal question is not how the monitors are instantiated and function but what kind of information they are monitoring.

From a legal point of view, in a situation where contractual policies need to be enforced[52] it is useful to monitor:

- **Procedures** (information exchanges with legal consequences);
- **Quality of Service parameters**
- **Events** (that lead to contractual breach or document the contractual breach)

TrustCoM WP8 has provided detailed examples of the monitoring metrics. It is not aimed in this Chapter to look into them once again. Instead, taking as a starting point the two GVOA examples provided in the Appendixes we could examine the main contractual policies and emphasize the monitoring requirements of some of them. It is to be remembered that not all the terms of a legal document can be translated at this point into objective metrics so as to automate and enforce in real time all the contractual policies. This would constitute a challenging objective in itself but it exceeds the scope of the description of work provided to TrustCoM. Given the current state of the art in TrustCoM it is possible to emphasize elements legally relevant that can be objectified and monitored in order to support the evidentiary process but not to replace it. During the litigation, other elements will have to be taken into account as well.

The legal input will be provided as a series of questions that would need to be answered in case a conflict arose among the VO Members. Those questions will

[52] More details about contractual enforcement can be found in Chapter 6 of this Deliverable.

be relevant not only in reviewing the completeness of the monitoring metrics provided in WP8 but would also in assessing which data from the one monitored and stored by TrustCoM needs to be retrieved and made available to the law enforcement authority at a certain point.

A. The first question to be answered is whether an agreement has been reached among the parties. The parties are bound to the terms of the GVOA only after the agreement has been concluded with all the required formalities. In this case we would need to determine:

    1) Have all the VO Members communicated their acceptance? (monitoring element: - acceptance message sent & received)

    2) If a deadline for communicating acceptance was provided, have all the acceptance messages been communicated in due time? (monitoring element: date of sending acceptance message)

    3) Have all the parties sent to the Notary the signed copies of the GVOA? (monitoring element: signed agreement sent/received)

B. Where a VO Member has suffered a reputation drop and he contests the grounds for such a decision:

    1) Is the reputation system working properly? (monitoring elements: the QoS parameters of the reputation system)

    2) Has a SLA breach has been recorded/ notified? (monitoring element: the SLA Status and ultimately SLA Metrics)

    3) Has a GVOA breach has been recorded/ notified? (monitoring element: GVOA status)

    4) Has that particular VO Member been responsible for the breach? (where/ who caused the breach)

    5) Has the liability of the VO Member been established beyond doubt?[53] (monitoring element: notification of liability sent/ received)

C. In case a confidentiality breach has been detected by one of the VO Members[54]:

    1) What confidential information assets are owned by each partner? (monitoring element: confidential information of one partner[55])

    2) What role is authorised to have access to them at a certain moment in time? (monitoring element: authorization tokens of each partner at one moment in time)

[53] This requirement basically prohibits the decrease in the reputation of a Service Provider as long as there still disagreement regarding its fault (as established by the definitive and irrevocable decision of the enforcement authority)

[54] for example, by realising that its confidential information has been accessed / is being used in a manner that was not authorised

[55] an evidence of all the confidential information owned by a party (and not by a role) can be kept only by an internal monitor

3) For what purposes? (monitoring element: authorization tokens of each partner at one moment in time) [56]

4) What was the status of certain confidential information at a certain moment in time (monitoring element: identity of the service provider who had access to a certain piece of information designated as confidential)?

D. A third party (not VO Member) is using pre-existing technology of a VO Member that was disclosed as part of the Project[57]:

1) Has the VO Member been notified about the disclosure to the third party? (monitoring element:notification of disclosure)

2) Has an acceptance of the disclosure been sent by the VO Member owner of the pre-existing technology? (monitoring element: acceptance of disclosure sent/received)

E. Force Majeure situations[58]:

1) Has the notification of force majeure been sent by the party affected by it? (monitoring element: notification of force majeure sent/ received)

2) Has the notification regarding the end of the force majeure situation has been sent/received? (monitoring element: notification of ended force majeure sent/ received)

3) How long has the force majeure situation lasted?[59] (calculated as the time interval among the delivery of the two notifications above)

F. Third party claims[60]:

1) Has the third party claim been notified to the VO Members and the VO Manager? (monitoring element: notification of third party claim sent/ received)

2) Has a claim for recourse been notified to the VO Manager and the responsible VO Member?[61] (monitoring element: notification of claim for recourse sent/ received)

G. Termination of the agreement:

1) Has a notice of voluntary termination[62] been sent/ received?

---

[56] what are the permitted actions for that role

[57] It refers to GVOA for the CE Scenario, Section 6 article 4(a).

[58] It refers to GVOA for the CE Scenario Section 8 article 4(b).

[59] It refers to GVOA for the CE Scenario Section 14 article 3(e).

[60] It refers to GVOA for the CE Scenario Section 9.

[61] It refers to GVOA for the CE Scenario Section 9 article 6(b).

[62] It refers to GVOA for the CE Scenario Section 14 article 2.

2) Has the voluntary termination produced delays or prejudice to the fulfilment of the project? (such as the ones arisen from the search for an appropriate replacement, an increase in the project costs…etc.)

3) Has a notification of breach of contract[63] been sent to /received by the Party to be expelled?

4) Has the Party in breach provided a remedy to the breach? (like for example by requiring a 3rd party to fulfil the obligation instead of it)

5) Has a notice of expulsion been sent to/ received by the Party?

H. Some of the learning resources selected to be part of a User's Learning Path are unavailable when needed:

1) Has the previous provider (according to the Learning Path) notified the subsequent provider[64]? (monitoring element: the Effective Date)

2) Has the notification of unavailability been sent by the LRP / received by the Portal Provider?[65] (monitoring element: notification of unavailability sent/received)

I. A user accesses Learning resources, subsequently it becomes apparent that the user was not authorised (shouldn't have had access)

1) When was the last authorised access of that user?

2) (When) did the Metacampus Portal Provider notify the LRPs that the User has ceased to be Authorised[66]? (monitoring element notification sent/ received)

3) Did the Metacampus Portal Provider notify the LRPs that an Authorised User has breached the terms of the End-User License[67]

As it can be observed from the questions above, most of the procedural elements that need to be checked during the evidentiary process in case of litigation refer to the sending/ receiving of a notification, informing the VO Members and/or the VO Host that a contractually relevant event has occurred. That notification marks the transfer of the contractual risks from the notifying VO Member to one or more of the VO Members, therefore placing the burden of proof either on the receiver of the notification or collectively on the VO.

[63] It refers to GVOA for the CE Scenario Section 14 article 3(b).

[64] It refers to GVOA for the AS Scenario Section 2 article 3 and 4.

[65] It refers to GVOA for the AS Scenario Section 2 article 5.

[66] It refers to GVOA for the AS Scenario Section 4 article 5 (c) (III).

[67] It refers to GVOA for the AS Scenario Section 4 article 5 (d).

6 Enforcement of VO Policies

The issue of enforceability of the policies comprised in the General VO Agreement arises in two situations:

- During the normal operation of the VO, when the VO Members interact in accordance with the terms and conditions they agreed to fulfilling the collaboration objective
- When culpably, negligently or for force majeure reasons one of the VO Members breaches the obligations he assumed via the VO Agreement.

One of the general principles of law[68] is that agreements produce effects (that is, giving rights and imposing obligations) only to the contractual partners[69]. As such, the provisions of the VO Agreement can only be imposed on those that are parts of the agreement, i.e on the VO Members for as long as the agreement is considered to be in force. Other parties- that somehow cause prejudice to either the VO Members or the VO Itself - could be stopped from doing so through legal means (remedies) that lie outside the contract.

This section of the study focuses on the enforcement of VO policies on the VO Members and aims at clarifying the correlation between the legal means for policy enforcement and the technical means of implementing and enforcing policies through the TrustCoM Policy Control Subsystem.

6.1 Automatic enforcement of policies

The automatic enforcement of policies concerns both the normal operation of the VO and the situations where breaches in the contractual obligations are detected. A detailed description of the Policy Subsystem is available in Section V of the Appendix B of the TrustCoM Framework Deliverable. In a simplified manner it can be said that access policies are enforced through evaluating the requests for access to each individual service against the policies that have been previously loaded onto Policy Decision Point of that service. For the enforcement of the obligation policies (ECA rules), notifications that are specified as being part of the policy[70] sent by the notifications broker are received by the policy service and then matched against the policies loaded onto it in order to assess the constraints specific for those policies. If the constraints are “true”[71] policy actions are executed.

---

[68] See for example Principles of European Contract Law (1995) available at:

http://www.jus.uio.no/lm/eu.contract.principles.part1.1995/

[69] With some distinctions that are beyond the scope of this analysis.

[70] Such as those listed in Section 5 of this Deliverable

[71] In accordance with Section VI.5 of the

From a technical point of view, it is not relevant whether or not the policies that are enforced are part of the normal operation of the VO or represent a reaction to contractual breaches. The architecture of the policy service permits the reuse of the generic ECA paradigm across various application scenarios. What differs is the source of the notifications (SLA Evaluator, the Reputation Service, the VO Manager or the Policy Enforcement Point) that lead to the activation of one or another policy.

6.2 Legal enforcement of policies

In the legal understanding of the notion, a contractual enforcement situation occurs where a contractual party (in our case a VO member) does not fulfil the obligations it assumed via the contract.

During the normal operation of the VO, the issue of “enforcement” does not come directly into play. We rather refer to the execution of the contractual terms, which assumes the voluntary observance of the contractual rules by the VO Members. Due to the fact that a signed Agreement is a legally binding instrument among the VO Members, all the message exchanges among them (and implicitly among the web services enabling the VO Members to collaborate) have to uphold the agreed terms and conditions. In the contrary, the VO Members (entities with legal personality) will be considered liable, which creates the premises for the activation of sanctionatory policies (described again in the GVOA) to be enforced either automatically or with human intervention.

Although it is desirable that the majority of the VO Policies become enforced with as little human intervention as possible and in real time (without interrupting the system’s functioning) in some instances some human involvement cannot be avoided:

(a) When the Policy Subsystem malfunctions;

(b) When the automatic enforcement is impossible since no policy was envisaged for the given situation

(c) When the enforcement of policy requires the interpretation of subjective circumstances or parameters

(d) When one of the parties contests the decision taken through automatic enforcement based on the intervention of circumstances that were not considered in taking the automatic decision.

(e) When the policies constrain the behaviour of the VO Members during the VO Lifecycle but offline

6.2.1 Malfunctions in the Policy Subsystem

In case the wrong policies are enforced by the Policy Subsystem, it is likely that the decision/ action will be contested at least by the VO Member mostly affected by the decision, or the VO Manager. In simple cases (for example where prejudice has not resulted from the activation of the wrong policy), the matter can be resolved

amicable within the VO. If prejudice occurred, the parties may still be able to tackle the consequences of the malfunction, but in some cases the matter may be referred to a law enforcement authority outside the VO. The enforcement authority will use a procedure that can be assimilated to the activity of the PDP, i.e. by comparing the agreed policies (the default rule) with the situation occurred in the specific case and taking compensatory measures (stipulated in the GVOA or dictated by equity).

6.2.2 Unpredictable circumstances

It cannot be assumed that all the businesses using the service oriented architecture will have the required knowledge and skills to foresee all the situations in which policies (especially ECA rules) will need to be enacted. Although some support may be provided through the use of templates, through support in instantiating Internal Business Processes, unpredictable circumstances or unclear policies if contested by one of the VO Members will need to be referred to an external enforcement authority.

6.2.3 Interpretation of subjective factors

Since the GVOA contains all the rules to be abided by the VO Members throughout the entire Operation, Evolution and Dissolution of the VO (and not only those policies that may be translated into objective statements), it is to be expected that some of those policies (or declarative specifications) will involve the evaluation of subjective factors, thus call for an external enforcement instance.

This may be the case where the VO Members have so called “obligation of means”, that is instead of guaranteeing a certain result, they have to “use best endeavors”, assess circumstances “to the best of their knowledge”, act in “good faith”, collaborate with “utmost care and due diligence”. Such designations are not meant to be “machine readable” but they are common in the legal practice and virtually all legal agreements will contain at least dome of them. They permit a law enforcement authority to take into consideration subjective, circumstantial or equity related factors in assessing especially the degree of fault of the party in breach or the amount of damages to be awarded to the prejudiced party.

Although such formulations bear no meaning in a machine readable format, they will appear in a GVOA for those circumstances in which the enforcement of the policy rules will not be done automatically.

6.2.4 Additional exceptional factors

Again, this circumstance relates to extraordinary occurrences where the range of factors that need to be considered before taking policy actions as stipulated in the GVOA should be extended exceptionally beyond the terms of the agreement, however not in contradiction with its spirit (the intention of the parties). It may be envisaged that where a business reputation or the amount of compensatory damages to be paid needs to be estimated, the parties will wish to bring into play additional circumstantial factors than the ones stipulated by the agreement (which does not mean that their argument will stand in front of an enforcement authority).

6.2.5 Offline interactions among the VO members

Legal enforcement of the policies concerning the offline interactions among the VO Members rely almost exclusively on the legal enforcement means.

Policies such as that "prohibiting the direct or indirect engagement in negotiations or discussions with third parties regarding the object of the Project", the obligation to "pay royalties in respect of any products manufactured or sold by a VO Member which incorporate in whole or to any material degree any Project Technology" or on the contrary, the "right of the Learning Resource Providers to compile, contribute to or publish on his own terms any other work on a similar subject to that of the Course delivered to an end user through Metacampus" can only be enforced *ex post*, through legal means.

It should be noticed however, that the legal enforcement does not necessarily involve litigation in the traditional sense of the word. Alternative dispute resolution (ADR) solutions do exist, and although their study was beyond the scope of the legal research in TrustCoM it can be envisaged that such solutions can be integrated in service oriented architecture like the one developed in the current project. Online dispute resolution (as a form of ADR) i.e the use of electronic communication for purposes of dispute resolution enable policy enforcement among parties situated in remote locations and produces an outcome which, just as a court decision is legally binding among the parties[72].

[72] for details about Online Dispute Resolution, state of the art and challenges, see Gabrielle Kaufmann-Kohler & Tomas Schultz, "*Online Dispute Resolution: Challenges for Contemporary Justice*", Kluwer Law International, 2004

7 Concluding remarks

The present Deliverable concludes the involvement of the Legal Workpackage (WP9) in an integrated research project aiming to create a trust, security and contract management framework enabling secure collaborative business processing in on-demand created, self-managed, scalable, and highly dynamic Virtual Organisations.

The legal research contributed to the definition of this framework regardless of whether we adopt the VO's view on the business processes (focused on the message exchanges between the service providers, without regard for the actual execution of the individual roles) or the view on the individual participants (describing the details per role and intermediate interaction partners, without insight into the overall process).

Our main achievements are[73]:

- We provided a legal perspective on the operation of the TrustCoM subsystems supporting the VO lifecycle. The interactions among the service components in each of the VO lifecycle were examined and mapped against the typical legal events corresponding to the same lifecycle phase
- We contributed to the conceptual models of TrustCoM through providing a contractual framework for the VOs and through explaining how VOs can use contracts to manage their interactions.
- We provided two possible instantiations of General VO Agreements corresponding to the two TestBed Scenarios developed in TrustCoM
- We introduced legal risk analysis as a novel inter-disciplinary approach for integrating of the perspectives of trust and security with the focus on legal issues related to virtual organizations.
- We ensured the integration between the different monitoring instances created as part of the TrustCom architecture (i.e at a Trusted Third party level, as well as Service Provider domain and host level) with the legal view on monitoring, notification and enforcement.
- We studied specific legal issues with major implications for the functioning of the VOs, such as jurisdiction and choice of law, access rights management, confidentiality and described legal requirements to be implemented during the interactions among the VO components of the lifecycle of the VO.

We should not omit some of the challenges we have faced during the studies: The research started with rather abstract legal questions which were more conceptual then application scenario oriented. Subsequently we identified legal requirements that should be considered when describing the behaviour of the business roles during the operation of the VO according to the two TrustCom Scenarios.

[73] This list of achievements follows a logic approach rather than a chronological one. For a chronological view of the achievements of WP9 in TrustCoM, please refer to the Introductory Section of this Deliverable

In choosing this approach we temporarily prioritised the definition, selection and analysis of the legal concepts we considered to be relevant during the operation of the VO over the legal analysis of the functioning of the Subsystems developed by TrustCoM or the contractual and policy requirements that would need to complement their deployment.

Subsequently, as a reflection of the advances in the TrustCoM framework as well as in the design of the Collaborative Engineering and the Aggregated Services Testbed Scenarios we could perform a more focused legal research and to suggest alternative or supplementary interactions among the TrustCoM subsystems.

The main challenges encountered in performing the current legal research arose however from its interdisciplinary character. Since all research areas have a long established and a clear-cut terminology, the meeting between the technical and the legal field generated inevitable conceptual clashes. Additionally, two distinct views regarding the VO lifecycle needed to be accommodated, one focusing on service interactions and another one on the interactions among entities with legal personality.

We are currently not aware of the existence of a Methodology or of some Best Practice Principles that could help smooth the integration of the various research philosophies. As a consequence, the compromise solution was a “learning by doing” experience.

Considering the limited scope of the TrustCoM Project, the list of legal challenges that we addressed here is not exhaustive. Based on the experience gained through the present collaboration, in the deployment of legally compliant web service solutions further legal support could be provided especially in the area of SLA Negotiation, Policy Enforcement and Evidentiary Processes in an Online Dispute Resolution context.