Deliverable

17

Legal risk management for Virtual Organisations

WP9 Legal Issues

Fredrik Vraalsen, SINTEF

Tobias Mahler, NRCCL
(eds.)

9 February 2006

Final Version

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 .

© Copyright 2005 Atos Origin on behalf of the Trustcom Consortium (membership defined above).

Neither the Trustcom Consortium, any member organisation nor any person acting on behalf of those organisations is responsible for the use that might be made of the following information.

The views expressed in this publication are the sole responsibility of the authors and do not necessarily reflect the views of the European Commission or the member organisations of the Trustcom Consortium.

All information provided in this document is provided 'as-is' with all faults without warranty of any kind, either expressed or implied. This publication is for general guidance only. All reasonable care and skill has been used in the compilation of this document. Although the authors have attempted to provide accurate information in this document, the Trustcom Consortium assumes no responsibility for the accuracy of the information.

Information is subject to change without notice.

Mention of products or services from vendors is for information purposes only and constitutes neither an endorsement nor a recommendation.

Reproduction is authorised provided the source is acknowledged.

IBM, the IBM logo, ibm.com, Lotus and Lotus Notes are trademarks of International Business Machines Corporation in the United States, other countries or both.

Microsoft is a trademark of Microsoft Corporation in the United States, other countries or both.

SAP is a trademark of SAP AG in the United States, other countries or both.

'BT' and 'BTexact' are registered trademarks of British Telecommunications Plc. in the United Kingdom, other countries or both.

Other company, product and service names may be trademarks, or service marks of others. All third-party trademarks are hereby acknowledged.

Deliverable datasheet

Project acronym: TrustCoM

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

Action Line: 6

Activity: Analysis of Legal Issues

Work Package: 9

Task:

Document title: Legal risk management for Virtual Organisations

Version: 3

Document reference:

Official delivery date: 31 January 2006

Actual publication date: 9 February 2006

File name: D17_main_report_V3.doc

Type of document: Report

Nature: Public

Authors: Dana Irina Cojocarasu[Error! Bookmark not defined.], Tobias Mahler[Error! Bookmark not defined.], Xavier Parent[Error! Bookmark not defined.], Bjørnar Solhaug[Error! Bookmark not defined.], Fredrik Vraalsen[Error! Bookmark not defined.]

Reviewers: CCLRC and Atos Origin

Approved by:

Version	Date Date	Sections Affected
V1	31/01/06	All.
V2	02/02/06	All.
V3 (final)	09/02/06	All.

Table of Content

1 EXECUTIVE SUMMARY 5

2 INTRODUCTION 8

3 TRUSTCOM CONTRACT MODEL 9

3.1 EN Contract 10

3.2 VO Contracts 11

3.3 Contracts and the VO lifecycle 12

3.4 Examples from the TrustCoM test bed scenarios 12

3.5 Drafting EN and VO contracts 13

4 SUMMARY OF METHOD AND LANGUAGE FOR LEGAL RISK MANAGEMENT 14

4.1 Risk management method 15

4.2 Graphical language 16

5 LEGAL RISK ANALYSIS OF ACCESS RIGHTS MANAGEMENT IN E-LEARNING SCENARIO 20

5.1 Access rights management 20

5.2 Access Rights Management in the eLearning Scenario 22

5.3 Legal Risk Analysis 24

5.3.1 Exceptions in national copyright laws 25

5.3.2 Misconfiguration of access policies 25

5.3.3 Trust 26

6 CONCLUDING REMARKS 27

7 APPENDICES 28

7.1 A. Method and language for legal risk management 28

7.2 B. Legal Risk Analysis of AS Scenario with respect to Access Rights Management . 28

7.3 C. Access rights management from a legal perspective 28

1 EXECUTIVE SUMMARY

This report summarises the research performed in TrustCoM work package 9 in the second half of 2005. The objective of TrustCoM's legal work package is to study selected legal issues in relation to trust, security and contract management for virtual organisations.

The present study's focus is on the legal risks in relation to access rights management, based on the ad-hoc dynamic services (AS) test bed scenarios developed in TrustCoM. Legal risk analysis allows this study to have a proactive approach on legal issues, which can be seen as opposed the reactive perspective inherent in traditional legal methods. Moreover, legal risk analysis facilitates the integration of the perspectives of trust and security with the different levels of contracts for virtual organisations.

TrustCoM has followed an approach in which two classes of VO contracts are defined:

- *VO Contracts*: contracts that express the general rules that each partner of a VO must abide to. These general rules for of collaboration constitute the legal basis for the collaboration. They define how the VO collaborates towards the achievement of the common goal and how the partners jointly work with reducing the risks of collaboration.
- *Service level agreement (SLA)*: contracts that express the specific rules that partners involved in a specific (operational) business process must abide to, for instance Quality of Service (QoS) requirements for a specific service.

These contract types need to be related to the different organisational levels of collaboration. The creation of VOs may be facilitated by an Enterprise Network (EN), which is set up as a basis for more specific collaboration in VOs. This EN will and should also be based on a contract which should include rules about the collaboration at EN level and about the creation of VOs. Hence, if there is a contract-based EN, both VO contract and SLAs may be understood within the context of the EN contract.

EN contracts will be defined by the EN, based on the types of VOs envisaged by the network, taking into account the specific needs of the industry in question and based on the requirements laid down by the applicable national laws. Though templates and model contracts are available, it is not possible to draft one general EN contract for all domains. There will be major differences between possible networks in various industries, services, jurisdictions, etc. However, the more similar the VOs in the network are, the more details may be included in the EN contract.

A particular challenge in relation to VOs is the speed with which they may be expected to be formed, potentially on a time scale on the order of minutes or seconds. Creation and signing of VO contracts may thus need to be fully automatic. The drafting of some elements of the EN or VO contract will be based on the business plan and strategy, on the specific needs of the industry in question, and

on specific requirements laid down by the applicable national laws. Moreover, the EN or VO contract needs to take into account risks related to the collaboration. This aspect can be covered in a legal risk analysis, which seeks to identify risks related to the collaboration, affecting either the common business goal or the assets of the participants.

To reduce the risks involved with establishing, joining and operating a VO, an approach for analysing and managing legal risks is needed which takes into account both technical and non-technical aspects. One of the goals of TrustCoM WP9 has been to develop methods and languages to facilitate legal risk analysis. These have been based on the existing CORAS model-based security risk analysis method and graphical threat modelling language. The updated risk analysis method, described in Appendix A, provides guidelines for identifying, prioritising and treating risks that can be addressed within an EN or VO contract. In addition, a simple checklist has been created for legal risks and treatments.

Risk analysis requires a clear understanding of the system or organisation to be analysed. The analysis typically involves a number of structured brainstorming sessions aimed at identifying and analysing risks and treatments. The effectiveness of such sessions depends on the extent to which the participants are able to communicate with and understand each other. We therefore propose the use of a graphical language for legal risk analysis, based on the CORAS graphical language for threat modelling. The language covers notions like asset, threat, risk and treatment, and supports communication among participants with different backgrounds through the definition of easy-to-understand symbols associated with the modelling elements of the language. Extensions for modelling legal issues have been made both to this graphical language and the Unified Modelling Language (UML), as described in Appendix A.

Since legal issues to a certain extent depend on the specific context, including the nature of the collaboration and its purpose, the legal research also focuses on issues of relevance to the scenarios selected by the project. In the context of the eLearning scenario, this study analyses the legal framework for access rights management, including WIPO Copyright Treaty and European Directives such as the Copyright Directive and the Conditional Access Directive. This legal framework is relevant for the TrustCoM eLearning scenario, which describes a collaboration of content providers, an eLearning portal and an infrastructure provider, who jointly provide eLearning services to different end-users in different countries.

The legal study on access rights management aims at integrating the operational features of the TrustCom AS architecture and business processes within the normative framework that constrains the actors' business behavior. The research goal is achieved first of all by presenting the relevant legal provisions regarding access rights in the EU legislation (which is done in detail in Annex C) and then by conducting a legal risk analysis evaluating possible risk scenarios having the Metacampus Portal Operator or the various Learning Content Providers as stakeholders. Hence, the proposed method and language were used in a case study of the TrustCoM eLearning scenario, with a focus on access rights management throughout the VO lifecycle, including liability aspects. The analysis is based on the assumption that these collaborators will utilize elements of the

TrustCoM architecture and framework in order to manage the access to eLearning resources. Appendix B of this deliverable reports on the results of this legal risk analysis.

The economic viability of the service provided as well as the reputation of the actors involved depend on the smooth clearance of access rights and on the effective protection against unauthorised access to the learning resources.

Legislation on Intellectual Property Rights provides for an obligation to require the authorisation of the rightholder prior to the desired use (access included) involving the protected content. The right to exclude others from accessing a protected content is doubled by the legal protection of the technology enabling the restriction on access. According to the EC Copyright Directive, the technological measures used by the author in connection with the exercise of his rights should be protected against circumvention.

A right to control access, however, can exist also in the absence of any IP rights of the beneficiary over the protected content. The author's access control rights, as stated by IP legislation, should be distinguished from similar rights awarded to the provider of an information society service whose economic viability (remuneration) depends on the use of an access control technology. In this case, similar to the interests of a cinema owner to obtain appropriate payment for the services provided, the interests of a service provider that makes his services available on request and makes use of access control mechanisms in order to ensure remuneration, are protected by laws implementing the Conditional Access Directive, regardless of the actual content of the service.

The individual rights management during the operational phase of the VO lifecycle, though circumscribed in the legal framework, occurs in accordance with the agreements reached in the initiation phase, more exactly by way of contractual licenses, which may be either exclusive or non-exclusive, and which may authorize one or all the uses. In accordance with the general principle of "freedom of contract" recognized in contract law, LCPs are free to transfer the access rights recognized to them by law to their contractual partner.

The legal risk analysis focused in part on the agreements and contracts that need to be created between the various actors: EN members, VO members and customers. These agreements control the activities and information flow during the different VO lifecycle phases.

The risk analysis was organised according to the typical lifecycle of a VO. We distinguish in general the following phases with respect to the lifecycle of a Virtual Organisation: Identification, Formation, Operation, Evolution and Dissolution & Termination. In some cases, like the one illustrated in this scenario, this lifecycle will be present both at the EN and at the VO level. Once the EN is formed, it will start to operate and to facilitate the creation of more targeted VOs (each VO with its own lifecycle). Even though the EN is much more stable than the VOs, its lifecycle may include the evolution of the network and it may even arrive at a stage of dissolution.

2 INTRODUCTION

This report summarises the research performed in TrustCoM work package 9 in the second half of 2005. The objective of TrustCoM's legal work package is to study selected legal issues in relation to trust, security and contract management for virtual organisations.

The present study's focus is on the legal risks in relation to access rights management, based on the ad-hoc dynamic services (AS) test bed scenarios developed in TrustCoM. Legal risk analysis allows this study to have a proactive approach on legal issues, which can be seen as opposed the reactive perspective inherent in traditional legal methods. Moreover, legal risk analysis facilitates the integration of the perspectives of trust and security with the different levels of contracts for virtual organisations.

The objectives of the research included in this study are to

- Contribute 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.
- Define 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.
- Evaluate this method and language based on the experiences with the scenarios studied in TrustCoM.
- Apply the method and language to the study of access rights management issues in the context of the TrustCoM eLearning scenario. This requires 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.
- Target the legal risk analysis to the VO lifecycle addressed in the TrustCoM framework.

In order to improve the readability of the document, this main report only includes brief summaries of the more detailed research, which is contained in the Appendices A, B and C.

- Appendix A describes the method and language for legal risk analysis, including its evaluation based on the studies so far undertaken in TrustCoM.
- Appendix B includes the legal risk analysis, which was used both to identify legal risks and treatments relevant to the phases of the VO lifecycle and to evaluate the suitability of the tools, method and language.
- Appendix C gives an account for the legal background for access rights management in the context of access to IP protected content.

3 TRUSTCOM CONTRACT MODEL

Virtual Organisations as envisaged by TrustCoM can be regarded as the coordinated collaboration between business entities that share a common goal. From a legal perspective, the virtual organisation will normally not be considered as an organisation with legal personality, but as an instance of collaboration between the VO members. The key means to steer this collaboration is a contract or a set of contracts between the participating organisations. These contracts play a vital role in governing commercial interactions between organisations. Moreover, the contracts need to be closely linked to business processes in the e-business applications. This interplay between the legal level and the business process level is necessary in order to facilitate the joint approach towards the achievement of the common goal and to reduce inherent risks. This integration is facilitated through the TrustCoM concept of General VO Agreement (GVOA). The GVOA is a "container" of VO contracts, SLAs and policies that all partners agree to.

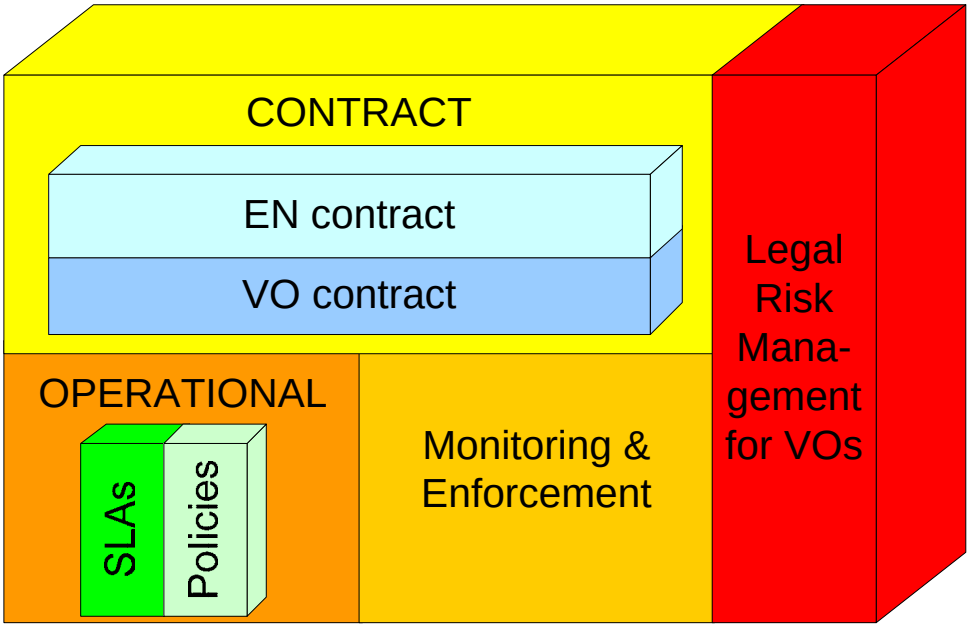


Figure 1: The Contract Model in TrustCoM

A contract is often defined as a legally binding agreement that creates an obligation to do or not to do a particular thing.[1] In the context of the TrustCoM project, our focus is on the internal legally binding agreements between VO participants.[2]

[1] William P. Statsky, *West's legal thesaurus/dictionary,* West Publ., St. Paul 1986. One may want to add that the contracts also may contain permissions.

Whether agreements between (prospective) VO participants can be considered as contracts, depends on whether the parties regard them as legally binding and enforceable. A contract is usually formed by an offer and an acceptance; sources of law (national or international) provide detailed requirements on contract formation.[3]

TrustCoM has followed an approach in which two classes of VO contracts are defined:

- *VO Contracts*: contracts that express the general rules that each partner of a VO must abide to. These general rules for of collaboration constitute the legal basis for the collaboration. They define how the VO collaborates towards the achievement of the common goal and how the partners jointly work with reducing the risks of collaboration.
- *Service level agreement (SLA)*: contracts that express the specific rules that partners involved in a specific (operational) business process must abide to.

A VO contract identifies and specifies the general rules that characterise how operational business processes are to be conducted through collaboration in a VO. On the other hand an SLA describes Quality of Service (QoS) objectives for a specific service as agreed by the service provider and the service consumer.

These contract types also need to be related to the different organisational levels of collaboration. The creation of VOs may be facilitated by an Enterprise Network (EN), which is set up as a basis for more specific collaboration in VOs. This EN will and should also be based on a contract which should include rules about the collaboration at EN level and about the creation of VOs. Hence, if there is a contract-based EN, both VO contract and SLAs may be understood within the context of the EN contract.

3.1 EN Contract

The EN contract will be drafted by the EN founding members; it will be formulated in natural language.

A template for an EN contract is included in the Report Legal Issues in SME clusters, provided by the Legal-IST project (legal-ist.org). An EN contract should at least cover basic issues for collaboration, including

- EN structure
- EN governance (EN management structure, etc.)
- Outline of VOs (industry domain, VO management, etc.)
- IPR & confidentiality issues

---

[2] There will also be contracts involving VO members and third parties, see e.g. Report on Consumer Protection and contracting with 3rd parties by the ALIVE IST project http://www.vive-ig.net/projects/alive/Documents/Consumer_Protection.zip.

[3] As an example, consider the United Nations Convention on Contracts for the International Sale of Goods (CISG) Article 14 I (1) and Article 18 I, even though they address goods and not services.

- Data protection issues, if applicable
- Payment & Costs,
- Liability and insurance
- Jurisdiction & Choice of Law
- Dispute settlement
- Etc.

EN contracts will be defined by the EN, based on the types of VOs envisaged by the network, taking into account the specific needs of the industry in question and based on the requirements laid down the applicable national law. 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. The more similar the VOs in the network are, the more details may be included in the EN contract.

3.2 VO Contracts

VO contracts may be written in natural language, but other formats may also be used. The content of VO contracts essentially depends on the specific kind of collaboration and on the relevant industry, (e.g. collaborative engineering in the aerospace industry or provisioning of eLearning services). A VO contract template in natural language was provided by ALIVE IST project (consortium agreement type of contract). More specific model contracts for different contexts are available in legal literature.[4]

Amongst the issues to be addressed by the VO contract are QoS requirements, access rights to computational resources, and trust issues (including consequences of one VO partner's trust level falling below threshold).

A particular challenge in relation to VOs is the speed with which they may be expected to be formed, potentially on a time scale on the order of minutes or seconds. Creation and signing of VO contracts may thus need to be fully automatic.

The creation of VO contracts may be facilitated through the use of templates drafted e.g. at EN level. EN members from a certain industry (e.g. collaborative engineering) will normally have access to typical contract models utilized in their industry. Based on these typical contract models, VO contract templates can be drafted by the EN founding members. In cases where there are major differences between VO contracts in an EN, the EN may need to draft several different VO contract templates. Some of these templates may be very detailed, leaving only some specific matters (e.g. QoS requirements and price) for the actual contract negotiation. The degree to which the VO templates need to be adapted depends on how much the VO contracts differ from each other.

[4] See, e.g., Richard Morgan and Kit Burden, *Morgan and Burden on computer contracts,* 7th edition Sweet & Maxwell, London 2005.

3.3 Contracts and the VO lifecycle

The EN and VO contracts will also need to address the different phases of the VO lifecycle: Firstly, in the pre-contractual stage of the VO (identification and formation), there may be preliminary contracts (letter of intent, memorandum of understanding/preliminary contract) regulating the creation of the VO.[5] At the same time, the EN contract may include rules for the creation of VOs, e.g. regarding the selection of prospective partners, confidentiality duties, etc. Secondly, the operation as well as the evolution of the VO will follow the rules laid down in the EN and/or VO contract. Thirdly, the dissolution of the VO will need to follow the contractual rules, and VO contracts will typically include rules about the effects of termination of the VO contract.[6] A VO contract may e.g. include confidentiality duties which will prevail even after dissolution. Similarly, liability issues may need to be addressed after dissolution. Last not least, if the VO is expected to generate results that may be IP protected, then the VO contract should address IP rights and use by VO members after dissolution. Hence, though the VO is dissolved, some contract provisions will remain valid and will require the attention of the VO partners. The contract should therefore be available for VO partners also after dissolution.

3.4 Examples from the TrustCoM test bed scenarios

The TrustCoM test bed scenarios illustrate that there will be major differences between VO contracts in different industries: The eLearning scenario envisages that there will be a Metacampus EN contract, i.e. a rather stable contract for those participating in the marketplace. In this scenario, VO formation needs to happen in a matter of seconds or minutes as the user requests and then selects a learning path via the portal. Since the VOs only differ with respect to the learning paths, the involved LCPs and end-users, most legal issues may be covered in the EN contract. Content providers could, for example, join the EN and agree to be bound by the EN contract when registering their services in the eLearning EN. Nevertheless there is a need for a (rather operational) eLearning VO contract that governs the provision of eLearning services to one end-user, based on one learning path. Contract templates could be specified e.g. by the initial eLearning EN founder(s) and agreed to by each EN partner as they join the EN. This would need to be anchored in the EN contract.

In the CE scenario, VOs will differ markedly from each other: Therefore, the EN will either be a rather loose club of collaborators, or there will be a multiplicity of ENs, or the EN is centralized around the CE VO. Nevertheless, there will probably be more stable contractual relations

- between the CEVO and the Air VO, on the one hand,
- between the CE VO and a group of (potential) service providers, on the other hand.

---

[5] See, e.g. ALIVE IST Project *VE Model Contracts, Deliverable D 17a* (2002), Section 3.

[6] For further details see ibid, Section 4.6 on p. 27.

The VO contracts between CE VO and other participants will differ based on the type of contract, e.g. outsourcing, ASP, consultancy, software licenses, combined contracts, etc. Model contracts and guidelines for the different contract types are available in legal literature.[7]

3.5 Drafting EN and VO contracts

EN and VO contracts will be drafted based on an assessment of the planned collaboration at EN and VO level. This assessment should both cover positive aspects (what is the business objective of the EN/VO and how can it be achieved) and negative aspects (risks related to the collaboration, affecting either the common business goal or the assets of the participants).

The drafting of some elements of the EN or VO contract will be based on the business plan and strategy, on the specific needs of the industry in question and on specific requirements laid down the applicable national law. This positive assessment will take into account the envisaged VOs the VO lifecycle, the VO management structure and what in TrustCoM is referred to as the collaboration definition. The collaboration definition includes a description of the involved actors, specified as business roles, and restrictions on such actors.[8] This information constitutes the input to define a VO contract.

Moreover, the EN or VO contract needs to take into account risks related to the collaboration. This aspect can be covered in a Legal Risk Analysis, which seeks to identify risks related to the collaboration, affecting either the common business goal or the assets of the participants. These risks may be identified and analysed in a structured way. This analysis results in a list of risks, which may be prioritized according to their likelihood and consequence value. This risk assessment serves as a basis for the drafting of rules in the EN or VO contract. Moreover, legal risk management serves as a bridge between the contract level and the operational technological level, including monitoring and enforcement. In particular, legal risk management may be utilized in order to

- Identify risks that need to be taken into account when drafting the EN or VO contract, including risks related to policies specified as described in the TrustCoM framework;
- Identify issues of high importance within the operational part of the GVOA;
- Identify risk areas that should be monitored and rules that need to be particularly enforced.

[7] Ibid.

[8] For details see Deliverable D 29_31_36 TrustCoM Framework.

4 SUMMARY OF METHOD AND LANGUAGE FOR LEGAL RISK MANAGEMENT

Businesses face an increasing number of security risks in the online world, and these risks are not limited to being of a technical nature. At an enterprise level, technical aspects of security are tightly interwoven with other aspects such as trust and legal issues. This is particularly true for the new breed of networked, virtual organisations with their dependency on information and communication technology for performing their daily work. This is further exacerbated by the international nature of many VOs, as well as their dynamic nature, where participants can join and leave the VO at different times during its lifetime.

There is no general European legal framework for the establishment and operation of virtual organizations. VOs therefore need to establish a clear contractual framework, which should regulate all relevant aspects of the collaboration. A recently published *strategic roadmap for advanced virtual organizations* points out that the analysis of legal risks arising in operating VOs and the development of legal strategies to overcome them is an important research task in order to support collaborate networked organizations.[9]

To reduce the risks involved with establishing, joining and operating a VO, an approach is needed for analysing and managing legal risks which takes into account both technical and non-technical aspects. One of the goals of TrustCoM WP9 has been to develop methods and languages to facilitate legal risk analysis. These have been based on the existing CORAS model-based security risk analysis method and graphical threat modelling language. A number of risk analyses have been performed of various legal aspects of the TrustCoM scenarios using the CORAS approach. The work in WP9 has hence focused on application and adaptation of the CORAS language and method to the integrated analysis of security, trust and legal issues[10,11,12], as well as continuous improvements of the language based on experiences from use and empirical investigations. The updated method and language are described below and in more detail in Appendix A.

---

[9] Luis Camarinha-Matos and Hamideh Afsarmanesh, *Collaborative networked oganizations: a research agenda for emerging business models,* Springer, New York 2004, p. 296.

[10] Brændeland, G., Stølen, K. (2004). *Using risk analysis to assess user trust – A net-bank scenario.* In Proceedings of the 2nd International Conference on Trust Management (iTrust '04). Oxford, UK. Springer LNCS 2995.

[11] Vraalsen, F., Lund, M. S., Mahler, T., Parent, X., Stølen, K. (2005a). *Specifying Legal Risk Scenarios Using the CORAS Threat Modelling Language – Experiences and the Way Forward.* In Proceedings of the 3rd International Conference on Trust Management (iTrust '05). Paris, France: Springer LNCS 3477.

[12] Mahler, T., Vraalsen, F. (2005). *Legal Risk Analysis with Respect to IPR in a Collaborative Engineering Virtual Organization*. In Proceedings of the 6th IFIP Working Conference on Virtual Enterprises (PRO-VE'05). Valencia, Spain: Springer.

4.1 Risk management method

The CORAS risk management method is based on the AS/NZS 4360 standard for risk management[13] and integrates aspects from different risk analysis techniques with state-of-the-art system modelling methods based on UML 2.0 (OMG, 2005a), the de facto standard modelling language for information systems.. *Risk management* is the sum of the culture, processes and structures that are directed towards effective management of potential opportunities and adverse effects. The *risk management process* consists of systematic application of management policies, procedures and practice to the tasks of establishing the context and identifying, analysing, evaluating, treating, monitoring and communicating risks. Risk management thus covers the entire lifecycle of the system or organisation, and may include several risk analyses with different focus areas and abstraction levels as the system or organisation and its surroundings evolve over time. The risk analysis process is typically organised as a set of meetings, as summarised in Figure 2 below.

A number of improvements have been made to the method description, and reusable elements have been created in the form of checklists for legal risks. The updated risk analysis process is described in more detail in Appendix A Section 3, while the checklists are presented in Appendix A Section 4. .

Meeting 1: Introduction
- Client present the system or organisation they wish to analyse
- Characterise the focus and scope for the analysis, including legal context
- Set up analysis plan

Meeting 2: High-level analysis
- Risk analysts present their understanding of the target of analysis
- Identify assets
- Establish initial threats and vulnerabilities

Meeting 3: Approval
- Target of analysis documentation
- Assign value to assets
- Identify risk evaluation criteria

Meeting 4: Risk identification
- Identify risks through structured brainstorming

Meeting 5: Risk estimation and evaluation
- Estimate likelihood and consequence of risks
- Evaluate risks with respect to risk evaluation criteria

Meeting 6: Risk treatment
- Identify and evaluate treatments

Meeting 7: Finalisation meeting (if necessary)
- Present results and get any missing input

Figure 2 Risk analysis meetings

[13] AS/NZS. (2004). *Risk Management*. AS/NZS 4360:2004. Australia. Standards Australia.

4.2 Graphical language

Risk analysis requires a clear understanding of the system or organisation to be analysed. This can only be achieved through the involvement of stakeholders and other interested parties with different backgrounds and knowledge about the system or organisation being analysed, e.g. decision makers, security experts, legal experts, system owners, developers and users. These participants are involved in the identification and evaluation of risks and treatments through structured brainstorming sessions.

The effectiveness of such sessions depends on the extent to which the participants are able to communicate with and understand each other. The CORAS graphical language for threat modelling[14] has been designed to mitigate this problem within the security domain. The graphical language is an extension of the UML 2.0 specification language. It is defined as a UML profile[15], and has recently become part of an OMG standard[16]. The language covers notions like asset, threat, risk and treatment, and supports communication among participants with different backgrounds through the definition of easy-to-understand symbols associated with the modelling elements of the language. A recent study has shown that the graphical symbols allow the participants to understand and read the diagrams more quickly[17].

[14] den Braber, F., Lund, M.S., Stølen, K., Vraalsen, F. (2005). *Integrating security in the development process with UML.* Encyclopedia of Information Science and Technology. USA: Information Resources Management Association.

[15] Lund, M.S., Hogganvik, I., Seehusen, F., Stølen, K. (2003). *UML profile for security assessment.* Technical Report STF40 A03066. SINTEF Telecom and informatics.

[16] OMG. (2005b). *UML Profile for Modeling Quality of Service and Fault Tolerance Characteristics and Mechanisms, Available Specification*. OMG Document: ptc/2005-05-02. Object Management Group.

[17] Hogganvik, I., Stølen, K. (2005). *On the Comprehension of Security Risk Scenarios*. In Proceedings of the 13th International Workshop on Program Comprehension (IWPC 2005). St. Louis, USA: IEEE Computer Society.

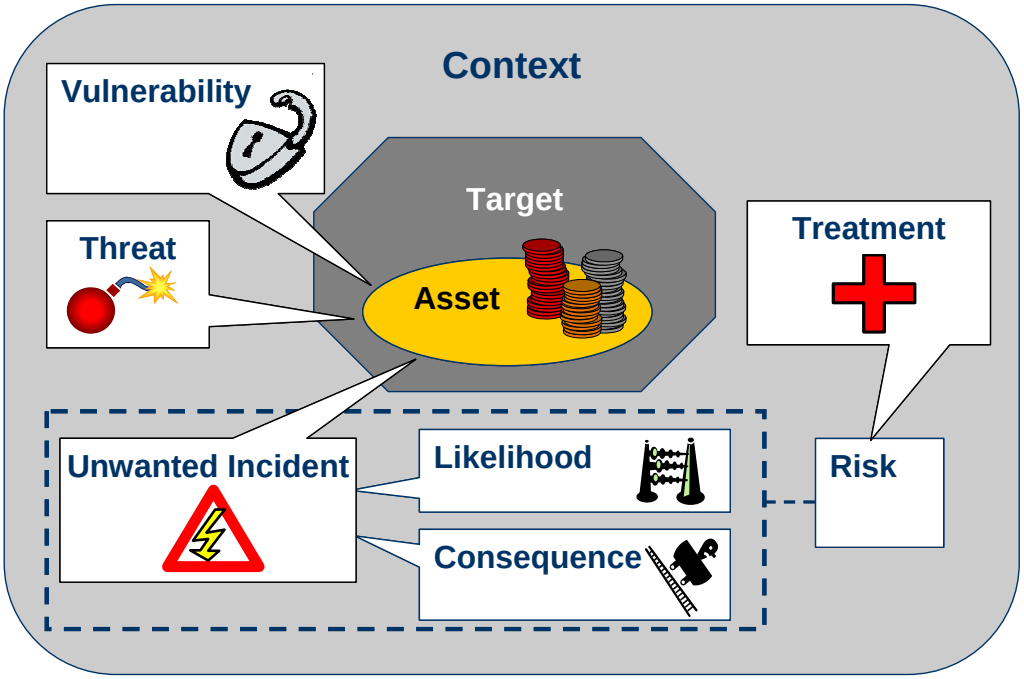
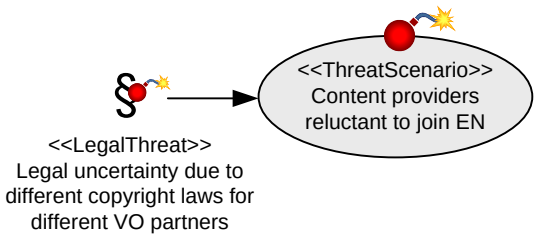


Figure 3 Elements of a risk analysis

Figure 3 shows the main elements of a risk analysis and gives examples of the symbols used by the graphical language. The *target* is the system or organisation, or parts thereof, which is the focus of the analysis. *Assets* are the parts or features of the target which have value to the client of the analysis, such as physical objects, know-how, services, software and hardware, and so on. A *vulnerability* is a weakness of the system or organisation. A *threat* may exploit a vulnerability and cause an *unwanted incident*, an event which reduces the value of one or more of the assets. A *risk* is an unwanted incident along with its estimated likelihood and consequence values. *Treatments* represent various options for reducing risk.

Facilities have been added to the graphical language to enable modelling of legal risks and treatments. An example of use of these new symbols is shown below in Figure 4, which is taken from the risk analysis of access rights management in the eLearning scenario presented in Appendix B.


<<ThreatScenario>>
Content providers
reluctant to join EN
<<LegalThreat>>
Legal uncertainty due to
different copyright laws for
different VO partners

6 CONCLUDING REMARKS

This work contributes to the overall TrustCoM framework

- by describing a possible contract model for Enterprise Networks and Virtual Organisations using the TrustCoM framework;
- by introducing a method and language for legal risk management, which will assist EN and VO members in the drafting of collaborative contracts with a particular focus on trust and security issues;
- by providing a method that bridges the different levels of contracts in VOs, including EN contracts, VO contracts and SLAs;
- by relating TrustCoM's focus on policies to the analysis of legal risks and, consequentially, to the drafting of VO contracts;
- by contributing to the clarification of the eLearning scenario through the collaboration with TrustCoM partners responsible for the TrustCoM test beds.

Since legal issues to a certain extent depend on the specific context, including the nature of the collaboration and its purpose, the legal research also focuses on issues of relevance to the scenarios selected by the project. In the context of the eLearning scenario, this study analyses the legal framework for access rights management, including WIPO Copyright Treaty and European Directives such as the Copyright Directive and the Conditional Access Directive.[28] This legal framework is relevant for the TrustCoM eLearning scenario, which describes a collaboration of content providers, an eLearning portal and an infrastructure provider, who jointly provide eLearning services to different end-users in different countries. It is assumed that these collaborators will use the TrustCoM framework in order to manage the access to eLearning resources. This deliverable therefore includes a legal risk analysis of the eLearning scenario, with a focus on access rights management based on the utilization of elements of the TrustCoM architecture and framework throughout the VO lifecycle, including liability aspects.

[28] See below Section 5.1 and Appendix C Access Rights Management.

7 APPENDICES

The following appendices are to be found in separate documents.

7.1 A. Method and language for legal risk management

7.2 B. Legal Risk Analysis of AS Scenario with respect to Access Rights Management

7.3 C. Access rights management from a legal perspective