Network of Excellence - Contract no.: IST-508 011
www.interop-noe.org

Deliverable DTG7.1

Roadmap for Interoperability and the Challenges of Non-Functional Aspects

Classification	Public
Project Responsible:	TG 7
Authors:	See below
Contributors	Task Group 7 members (see below)
Task	TG 7.1
Status:	Version 1.0 (TG7 v 1.7)
Date :	2005/11/24

Contributors

Rose-Mharie Åhlfeldt	HS (48)	nfa
George Athanasopoulos	NKUA (32)	trust
Panagiotis Bouros	NKUA (32)	trust
Yannis Cotronis	NKUA (32)	trust
Michel Deriaz	UNIGE (52)	trust
Vangelis Floros	NKUA (32)	trust
Michael Goedicke	UDE (31)	nfa(lead)
Michael Hatzopoulos	NKUA (32)	trust
Maria-Eugenia Iacob	TELEMATICA (43)	nfa
Henk Jonkers	TELEMATICA (43)	nfa(lead)
Vandana Kabilan	KTH (47)	e-contracts
Carsten Köllmann	UDE (31)	nfa
Eleni Koutrouli	NKUA (32)	trust
Lea Kutvonen	UHDCS (22)	trust(lead), e-contracts, nfa
Peter Linington	UNIKENT (51)	coordinating editor
Drakoulis Martakos	NKUA (32)	trust
Giovanna Di Marzo Serugendo	UNIGE (52)	trust
Jean-Henry Morin	UNIGE (52)	drm(lead)
Michel Pawlak	UNIGE (52)	drm
André Rifaut	CRPHT (42)	value(lead)
Sini Ruohomaa	UHDCS (22)	trust
Paolo Spagnoletti	LUISS (invited)	nfa
Aphrodite Tsalgatidou	NKUA (32)	trust
Hans Weigand	UNITILB (44)	e-contracts(lead)

Table of contents

Executive Summary

This deliverable defines a roadmap for future work on the special interoperability issues that arise from consideration of non-functional aspects of information systems. The roadmap will provide the structure for further activity in this area during the remainder of the INTEROP project and beyond.

Non-functional aspects are concerned with the many facets of quality of provision that arise in the real world. The primary objectives of a system can often be expressed by business goals and abstract business processes, but the system's fitness for purpose is based on many other things: its security, its performance, its value for money, and so on. Decisions about these aspects are generally not taken in isolation for a single business process, but form organizational policies that apply to the whole family of business activities within an enterprise. The key to managing non-functional aspects is the controlled separation of concerns from the business goals so that this commonality can be exploited.

All this is true of any system, but managing non-functional aspects in the context of dynamically created interoperation between separately owned and managed systems requires much more. It needs a clear analytical framework and an architecture for the open exchange of knowledge and for the descriptions and negotiation of options. It is these areas that are addressed here.

The work described here is a natural extension of the earlier state of the art analysis produced within the INTEROP work package on architectures and platforms (WP9); that work identified a broad area where solutions were needed, and this deliverable is the output of a new task group (TG7) that was formed to take the analysis to a further level of detail. To do so, it has concentrated on a number of focus areas that each represent particular interoperability challenges: trust, e-contracting, security, performance, digital rights and business value. This list covers a wide range of problems at different levels of abstraction, and combining them is a challenging test of the cohesion of the individual solutions.

The comparison of these focus areas has led to the identification of a number of common requirements that cut across the different aspects, and these common requirements illuminate the various steps in system specification and operation: modelling, analysis, platform provision and tool-based, model-driven development and deployment. All of these need to take non-functional aspects into account, and the current roadmap identifies required elements that enable this to happen in a coordinated way. It then identifies and positions a series of actions needed to progress the work.

The immediate consequence of this work has been to identify a number of pieces of joint work that are to be carried out within the task group. Doing so will test the conclusions of this roadmap and allow its framework to be refined further. The publication of papers based on these investigations will help both to validate the architectural assumptions and to disseminate information about these important elements of interoperability to a broader commercial, scientific and engineering community. Publication in the open literature, and thus being subject to the peer review processes associated with it, will result in a stronger validation of the work than an internal review could provide.

PART I – Overview of the Roadmap

I.1 Introduction

I.1.1 Background and Motivation

The interoperability of information systems owned by different organizations has been much studied and there is a general consensus that the key to interoperability is the establishment of shared knowledge to provide a firm basis for the control and interpretation of communication. Thus interoperability of business processes depends on the establishment of a single shared reference ontology from which detailed agreements and dialogue structures can be derived. However, there is much more to communication than the interpretation of messages directly in business terms; there are many further issues of quality, security, trust, ownership and business value that need to be considered in ensuring that the objectives of the cooperative organizations are, in fact, met.

The present document aims to move forward the understanding of how to handle these non-functional aspects during interoperation by creating a roadmap for this specific part of the problem, and identifying where new pathways need to be cleared to reach the general goal of forming effective and predictable e-Communities.

So, what, more precisely, are these non-functional aspects? The underlying motivation for introducing them is the well-known need for separation of concerns; there is generally a business process view of an activity, concentrating on the main behaviour of an enterprise and the applications that support it, but there are also other aspects that concentrate on different areas that can be specified largely independently, and these specifications are generally applied across a range of applications operated by the organization, and represent the broad policies it establishes.

The most common examples given are probably the quality of service and security requirements mentioned above. They can be specified largely independently of the functional behaviour, but this does not imply that these aspects can therefore be neglected. Considering them as separate concerns allows structuring of the design work, but it is important that all the different aspects are considered from the beginning of any system design, and that the resultant design should be considered and reviewed as a whole. This means that suitable frameworks and techniques are needed to manage all the facets of the resulting big picture.

In the past, the combination and reconciliation of the different aspects has often been left too late in the development cycle, leading to solutions that are both inadequate and difficult to change. Interoperability implies dynamic negotiation of new agreements about how the aspects are to be achieved in the resulting composite enterprise that is being created, and this demands planning from an early stage for the flexible creation and extension of agreements on how quality, in its widest sense, is to be maintained at the required level.

It is the creation of a framework able to express requirements and manage such general quality negotiations that is the main aim of the TG7 experts.

I.1.2 The Structure of the Roadmap

There is much to be said about the support of non-functional aspects, but the supporting detail may go beyond the interest of many readers. This roadmap is therefore divided into two parts. The first gives an overview of the objectives, the process, the areas studied and the main action points proposed. The second part gives general background material and then a sequence of detailed analyses of the five focus areas selected by TG7. The second part includes full references to supporting material in each area, but in the first part references are restricted to general tutorial material likely to be of interest to the more general reader without the time to spend on a more detailed study.

I.2 Producing the Roadmap

I.2.1 Earlier Work in INTEROP

At the start of the INTEROP project, the work package on Architectures and Platforms (WP9) undertook an extensive state of the art review, resulting in deliverable D9.1. One section of this review focused on the so-called *Non-Functional Aspects*, which were widely recognised as playing a key role in the creation of high value IT systems. The experts producing this review felt that there were many unsolved problems in the management of non-functional aspects during interoperation between separately owned and managed systems. They therefore took the initiative to propose and launch a new task group, TG7, chartered to take this work further.

This roadmap is a natural evolution of the work on non-functional aspects carried out in INTEROP WP9, extending its reach beyond the purely technical issues into the business and strategic levels of interoperability. The objective has been to achieve a high degree of integration with respect to the three major themes of INTEROP (Architectures and Platforms, Enterprise Modelling and Ontologies). Competencies have been drawn from partners already active in all three aspects of INTEROP, adding to it the insights from the more industrially oriented ATHENA project, and thus creating a productive synergy.

I.2.2 Selection of Action Areas

In defining the technical aims of TG7, the objective was to cover a broad range of non-functional aspects, while gaining the maximum benefit from the expertise of the partners involved. One of the challenges in placing the many aspects under discussion into a single unifying structure is the very wide range of levels of abstraction and the wide variety of modelling techniques used in specifying them. They extend from the very specific technology focus found in some aspects of quality of service, through to the broad management view taken in assessing business value. The aim was to make a selection that covered the whole of this spectrum.

The task was also formulated in the knowledge that many of the experts involved had interests in what might be termed the defensive aspects of organizational governance – trust, security, contracting and rights management. This emphasis gave an opportunity for identifying related themes that cut across the range of aspect types.

These considerations lead to the selection as specific focus areas of:

- trust and trust models; this area has been selected because it is central to the management of dynamic relationships between organizations, and thus underpins many aspects of interoperability;
- e-contracting; the idea of a contract is key to most business interactions, and the growing area of e-contracting enables the migration of many processes from the manual to the automated domain;
- representative classical non-functional concerns, specifically security and performance; these were selected to maintain the link with architectures and platforms – security was chosen because of the synergy with the other areas in this list, and performance as a representative quantitative aspect;
- digital rights management and associated organizational policies; the system-wide control of digital rights is a growing area of concern, and its emphasis on control at the point of use gives a counterpoint to security by encapsulation;
- business value; this links the details of process execution to broader considerations of risk and value associated with the processes performed and the resources they manipulate, and provides a basis for assessing organizational requirements and goals. Of the areas considered, it takes the most abstract view of the interoperating community.

I.2.3 Generating the Roadmap

The intended scope and content of the Roadmap were decided in a series of consultative meetings involving the INTEROP WP9 members, as a part of the formulation of the TG7 plan. The focus areas were agreed at this stage. Following a joint orientation session in the INTEROP workshop at Valencia, in which all the areas were presented and discussed, the main focus of the work moved to the individual areas. The five groups progressed independently, each producing a statement of the current knowledge and immediate issues for their area, highlighting, in particular, those issues that affect interoperability.

Although the five streams of work resulting from the focus areas progressed independently, their developing views were open to all members of the task group, and review and comment by the full group was encouraged at all stages. The outputs of the five streams were combined into a single partial draft shortly before the INTEROP workshop at Bologna, and more general issues identified and debated in that workshop. All members of the task group have had the opportunity to review and contribute to the resulting final draft.

The aim in creating this roadmap is to create an overview and identify a set of areas needing further work that will remain valid for several years. It brings together previous work on trust, security and other non-functional aspects within INTEROP and, by so doing, provides a framework and programme of work for activities during the remainder of the INTEROP Network's activities and beyond. It identifies a number of specific topics that bring out shared knowledge and encourage common activities of the task group members. The Roadmap aims to help the further development of these areas by making the definitions of the topics more precise, and by exploring the relationships between them and with other areas of the INTEROP activity. Doing this will help to clarify the objectives of the joint work, and help to make best use of the effort available by avoiding duplication and overlap of work.

The concluding section of this part identifies a number of focus areas in which task group activities are already being initiated, but the vision extends well beyond the lifetime of this project, and some of the actions needed will not even have been started during it.

I.2.4 Validating the work in TG7

It must be remembered that INTEROP is a Network of Excellence, and not primarily a research project. The Joint Research activities within it are funded at below marginal cost. The inclusion of research activities in this project is motivated by the need to engage in a process of synthesis and consolidation to ensure that the dissemination activities are sufficiently forward looking and to ensure that they do in fact attract the highest level of excellence and expertise.

The emphasis in this task group has therefore been placed on activities that fill gaps and on identifying new directions; the main deliverables following on from them are to be published papers. The quality of these papers will be tested by rigorous internal reviews, but the final guarantee of soundness and quality will be ensured by submitting them to the external peer review processes provided by reputable journals and conferences.

I.3 Overview of the Focus Areas

This section summarizes the main focus areas; more detailed descriptions and full references to previous work can be found in part II of this document. To avoid duplication and keep a clear focus, references in the summary are restricted to survey and introductory tutorial material. The actions required in the focus areas, or across the board, are brought together in the final two sections.

I.3.1.1 Trust and Trust Models

The introduction of integration of systems or collaborations between independent service components gives rise to considerations of trust and distrust between those components, their users, and the environment and context in which those components communicate.

Models and systems developed for supporting trust decisions and activities for trust management are concerned with a variety of dimensions: users trust the systems in use, enterprise systems and services trust each other, and finally, human and software users of the trust management system trust the society's infrastructure services for regulations, credential issuers, and identity management of trustees [GS00], [MC96].

Trust and reputation are complex, multifaceted notions expressing quantified belief that the trustee has named qualities, such as a certain behaviour, competence, accuracy of information or process, or integrity [RK05] [V05] [ZYI04]. Trust decisions can be taken on the basis of that belief leading to a variety of indications, depending on the application area. The main areas of interest can be captured by the large and overlapping themes of:

a) inter-enterprise collaborations and partnership;

b) exchange of information between users;

c) personalization of services, and

d) selection and restriction of services used.

The belief can be computed from a number of information elements, such as context information, action importance, risk involved, and past experience information. There is a strong expectation for trust to be a dynamic concept that provides for adaptation to new situations in the networked environment. There is no consensus so far on the set of information items or metrics for computing trust, or on the transitivity models for trust.

Trust management includes facilities for:

- initialization of trust information for a trustee,
- observing or measuring properties of the trustee and accumulating that information as trust or reputation values,
- use of trust information for trust decisions,
- management trust relationships (contracts) and delegations,
- managing and interpreting the integrity of trust and reputation information.

An essential aspect for trust management between enterprises is the dependability of the services they provide. The way that the platforms providing services and the communication facilities they use are secured is discussed in the NFA subtask. This subtask is primarily interested in a high-level view of trust, both within inter-enterprise collaboration and e-Contracting; and as an aspect of information exchange and composition.

I.3.1.2 e-Contracting

With the growing increase in Internet based commerce, business enterprises need to establish precise, unambiguous coordination of internal and inter-enterprise business processes. Various researchers have addressed the coordination of inter-organizational transactions from a contract perspective [RKKC04], [TT98], [DS97]. The term “contract” is used in two ways:

- *business*: an interorganizational business process often represents a business transaction or service level agreement and thus comprises a contract from a legal point of view. This contract contains the legal obligations on the parties involved in carrying out some value exchange.
- *technical*: in an interorganizational business process, we have to deal with the choreography or coordination of private business processes. It makes sense to separate these coordination aspects from the functionality of the applications (web services) involved. The term ”contract” is used metaphorically for the high-level description of the coordination aspects – whether this description has a legal status or not.

Contract-based interoperability can be defined as: “the ability of applications to interact and work together on the basis of a contract”, where a contract is defined as: “an agreement between two or more roles that governs their interaction in terms of obligations and permissions”. It is possible to consider different levels of contract-based interoperability, depending roughly on the automation level of contract establishment and the functionalities (e.g. transaction support) of the contract execution environment.

Specific Cross Cutting Issues to other Sub Tasks

- In contract establishment, business goals and operational trust between the contracting parties are key input parameters. This relates to the subtask *Business Value* and the subtask *Trust & Trust Models*, respectively. Another question is what the effect of an e-contract is on the trust level of the parties.
- Traditionally, e-contracting has been focusing on functional aspects. An interesting question is how to specify *non-functional requirements* in contracts.
- The enforcement and monitoring of e-contracts requires a capable technical infrastructure. As far as access rights are concerned, this question relates to the area of *Digital Rights Management*

I.3.1.3 Non-Functional Aspects

Current approaches to the design of interoperable systems have a strong focus on functionality. Non-functional aspects (NFA), such as security and Quality of Service (QoS), are often added as an afterthought. However, it is becoming more and more accepted that these aspect should be an integral part of the design process, from the global architectural descriptions to the detailed system specifications. In addition, concepts and infrastructure level facilities for managing non-functional aspects should become an integral part of the runtime and service development environments.

Many different non-functional aspects can be identified, which can be classified in aspects that are usually described in *qualitative* terms (e.g. security, trust and the different '-ilities') and aspects that are *quantifiable* (e.g., the various QoS properties and business value). The future joint research of the NFA subtask will focus on one representative aspect from each of these two classes: *security* and *QoS* (and in particular *performance*). This is motivated by the fact that these aspects best represent the shared interest of the partners involved, and they are not covered by the other specific subtasks.

Within this focus, three specific directions for joint research are envisaged:

1. **Design-time support for non-functional aspects** (in particular QoS). In the first place, this research is concerned with the question of how to model and analyse QoS properties at different levels of detail, both in the business domain and the technical domain. A second issue is the integration of the resulting models, which will require an extension of the prevailing Model Driven Development (MDD) techniques to cover the non-functional aspects [SE03], [JILS05]. This includes an extension of existing model transformation techniques, which requires close co-operation with InterOp TG3 (model morphisms). Possibly, techniques for aspect-oriented modelling ("model weaving") [SSR+05] and aspect-oriented transformations may prove useful here.
2. **Run-time support for non-functional aspects** (in particular QoS). This research should result in generic architectures and platform mechanisms to support the management of NFA/QoS at run-time. This includes, e.g., mechanisms for the dialogue structures and processes for the negotiation of service levels, and monitoring in enforcement facilities.
3. **Security management in service-oriented architectures**. The TFI framework looks at security management issues for Information Systems from the technical, formal and informal viewpoints (hence TFI), which are in continuous interaction. The InfoSec

model [ÅN05] has been developed to deal with information security issues. In this research, these models are compared to each other, and their combination and joint application is investigated in the context of service-oriented architectures and web services.

I.3.1.4 Digital Rights Management

As businesses and their processes are irrevocably engaged on the path of interoperation and virtualization, it is now mandatory for them to address the issue of the persistent protection and governed usage of corporate digital assets [BBGR03] [RTM01]. Those assets represent a strategic resource thus needing a managed approach to their security not only within organizations but also outside the corporate environment and its technical perimeter. Moreover, many emerging and future regulatory frameworks (such as SOX, Basel II, HIPAA, NASD, etc. – see part II) are becoming more and more important in daily operations and thus require near real time compliance monitoring.

Digital Rights Management (DRM) technologies represent the technical means to fulfil many of these requirements by providing the *last mile* of the traditional security stack. Of utmost importance in this context are two major challenges that need to be tackled. First, there is the interoperability challenge, which is an essential enabling factor for the creation of virtual organizations and processes spanning corporate and legal boundaries, and second, the strategic challenge of addressing such issues at the policy level. Digital Policy Management (DPM) represents the strategic dimension of the problem. It requires the ability to capture, model, represent, and assess internal and external policies governing the business prior to their digital instrumentation and deployment using Digital Rights Management technologies.

It is worth mentioning that the compliance issue is a problem that is here to stay, requiring a recurring audit activity in order to prove compliance. It is therefore vital for corporations to place this issue high on the agenda not only from a specific risk mitigation point of views but also, and more importantly, at the strategic level of corporate governance. This requires a consistent approach that is global to the enterprise, involving everyone at all levels, as well as defining accurate management dashboards for its continuous monitoring. Thus, Digital Policy Management becomes a strategic project under the supervision and responsibility of the top management. It will be only at this price that companies will be able to cope seamlessly with current and future policy and regulatory issues in a cost effective way.

I.3.1.5 Business Value

Interoperable systems that are built across different organizations must show their added value when compared to the systems that currently often co-exists within each organization engaging in some form of loose cooperation. In order to tackle this challenge, techniques must be created to assign a value to each system or system component making up the interoperable systems [OGP05] [GA01]. Often, when analysing the value of inter-enterprise business systems, the analysis is limited to the value of end-to-end business services that are implemented in those systems [HV99]. However, the value (in terms of cost/revenue) of non-functional aspects is an important part of the end-to-end business service. Moreover, the design decisions to implement these non-functional aspects impact on the cost/revenues, and also the high dynamic profile of non-functional aspects results in a dynamic profile for the value. In addition to this, the organizational environment is a primary factor determining the costs and revenues of complex business systems.

This is why the process of designing these systems has to consider the most important non-functional aspects that result in the value of the end-to-end services that the system implements. Currently model-driven design methods are the most promising methods for building large and complex interoperable systems.The research direction to be taken here concerns the introduction of techniques such as goal-oriented requirements engineering and risk analysis to support the concept of value in model-driven engineering method (including non-functional aspects).

One example of the addition of those techniques to model-driven engineering is presented in Figure 1. This example applies to a model-driven security engineering method.

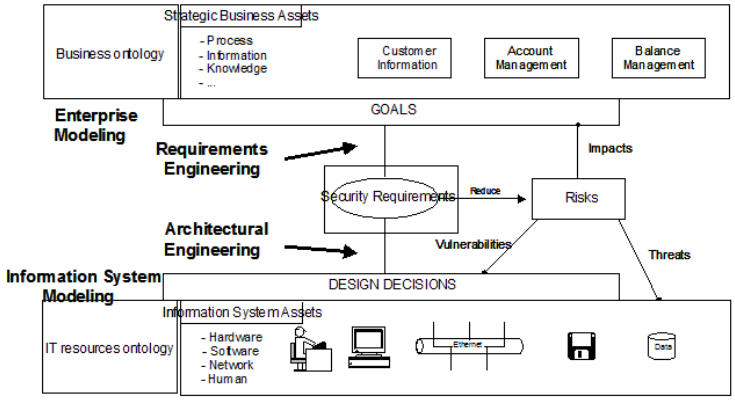

Figure 1: Goal-driven risk analysis for model driven security engineering

In this diagram, one can see that the goal-driven risk analysis incrementally drives the design choices via cost/benefit indicators. The value associated with each business asset (identified through an analysis of business models, using techniques of INTEROP Task Group 5) is associated with its goals. These goals are refined with model-driven techniques into security requirements and IT architecture, amongst others. The IT assets identified in the IT architecture have new values that must be taken into account and are introduced into the goal-driven risk analysis, possibly modifying the preceding design choices (introducing an optimisation cycle into the model-driven method). An ontology of business assets, IT assets, the non-functional aspects considered (e.g. security), goal analysis and risk analysis is at the heart of the method.

I.4 Planning Future Activities

A roadmap normally describes the relative positioning of important concepts and functions in some area, and identifies gaps in current work, so that the requirements for, and constraints on, future work items are made clear. It is in the nature of work on non-functional aspects that it is, to some extent, dependent on the style of the functional business processes to be supported; the roadmap needed here is therefore more an overlay than a completely independent map, and many of the structures and techniques already identified in INTEROP will be taken as the basis.

The approach here, therefore, is to identify a series of additional elements needed to relate the different aspects to each other and to the primary business processes. For each element we describe the objectives and the directions to be taken to achieve them.

I.4.1 Cross-cutting Actions

Before turning to the five focus areas, there are a number of requirements that can be found in any one of them. The following four cross-cutting activities have been identified as necessary to support all the individual focus areas. Progress in these areas is necessary to provide a scaffolding for the consistent development of solutions in the individual areas. The expectation within TG7 is that the same approach will also prove to be applicable to the broader range of non-functional aspects not studied in detail in this task.

I.4.1.1 A Coordinated Set of Aspect Models

Describing the required properties of a non-functional aspect generally involves constructing a model for the key entities and behaviours that constitute the aspect. Each aspect is, by definition, different, and so will need its own model, but some of them will overlap and the understanding of commonality and divergence of requirements will be easier if the modelling style chosen for each is similar, so that the models constitute a unified family. This family, taken together, will then form a key part of the shared reference ontology needed to support interoperability.

The aim of this action is to perform a comparison of the modelling requirements of the aspects of particular interest to TG7 and identify where and why they differ. It will then be necessary to perform a synthesis from the range of requirements to establish a common architecture and style, supported, where appropriate, by common templates or metamodels.

This action will have a strong symbiotic relationship both with the action on common supporting mechanisms, and with the action on the application of model driven techniques for system construction and maintenance.

I.4.1.2 Common Supporting Mechanisms

The process of establishing, between two organizations, an agreement to interoperate, and then of instantiating this agreement in actual interoperation, involves the creation of a shared context. This starts from the reference ontology but not only establishes information about the partners, but also, in general, extends the working ontology by agreeing specific refined definitions for use within the context that is being established.

This action will identify the basic mechanisms needed to support the creation (and ongoing maintenance) of the shared context. The mechanisms it is concerned with are centred on negotiation and knowledge dissemination. They will be defined in an abstract, platform independent way, but consideration of how they would be provided by some well-known platforms would be part of the supporting validation process.

It should be clear that the mechanisms are largely concerned with the manipulation of instances of the models defined in I.4.1.1, and that this is the source of the close relationship between the two actions mentioned above.

I.4.1.3 Requirements for Model Driven Development

Having taken the route of viewing the virtual organization we are creating in terms of a set of largely independent aspects, we are faced with the problem of how to weave these aspects together to form a complete working solution. The modern trend is to handle system realization in a model driven way, and this is no exception.

However, the weaving of non-functional aspects raises particular challenges for Model Driven Development. In contrast to the traditional Platform Independent Model (PIM) to Platform Specific Model (PSM) transformation template, a weaving process involves multiple controlling models (one for the business rules and one for each other aspect), and often needs to generate multiple target models, because the result will be not only the realization of an application, but also the creation of configuration definitions for, for example, firewalls or supporting publish and subscribe structures. This represents a considerable challenge for the modelling and transformation definition processes, since the transformation rules need to be expressed in a way that links multiple source and target domains.

This action will analyse the weaving requirements to identify the transformation styles that need to be supported, and the resulting facilities that must be present in general transformation languages.

I.4.1.4 Assessing the Maturity of NFA support

The whole field of research into interoperability is evolving very rapidly, and is resulting in a wide and diverse range of proposals for supporting platforms, tools and organizational structures. These each solve part of the problem, but need to be assessed in a holistic way to judge the capabilities and achievements over all. This is particularly the case when the added complexity of supporting the full range of non-functional aspects is taken into account.

What is needed is an agreed set of milestones along the route from manual interoperability to intelligent, autonomous creation of interoperability solutions on a dynamic basis. These milestones will need to be supported by clearly defined criteria to determine whether or not they have been reached, in whole or in part, in a particular situation. The milestones and associated criteria will need to be defined in a platform and process independent way.

This action will propose such a framework for assessing the maturity of interoperability solutions that support non-functional aspects. It will build on existing proposals made in the e-contracting area, and on the long established software engineering capability and maturity models of process. It has the potential for widespread application throughout this whole research area.

I.4.2 Individual Action Areas

The general action lines expressed above can be refined and extended in each of the specific areas addressed. The work on the individual areas will both test the validity of the general assumptions and feed back additional requirement to make the outputs of the cross-cutting activities more comprehensive and robust.

I.4.2.1 Trust and Trust Models

As the interoperability issues of trust are strongly dependent on the application area of interest, the group has identified two specific interest areas: inter-enterprise collaborations, and data integration.

The group has indicated interests in further work on:

- development of enhanced trust models for data exchange in P2P systems;
- reputation-based trust models of P2P systems; identifying challenges, interoperability issues, and designing a common trust model;
- development of an architecture and set of facilities that uses trust information as part of e-Contracting, and for e-Community monitoring and management.

These themes integrate well with all of the cross-cutting issues by addressing the coordinated set of aspect models. They do this by providing a reputation-based trust model for inter-enterprise situations; by providing ontology requirements for e-Contracts, and requirements for runtime mechanism such as negotiations, monitoring, and accumulating trust information.

Besides the cross-cutting issues, the group is interested on addressing privacy in data integration, ontologies for trust and reputation, and trust models for e-Services (web services).

I.4.2.2 e-Contracting

Some specific research objectives related to e-contracting that could be taken up in INTEROP are:

- to establish a framework for contract management - including evaluation/assessment both of individual contracts and at the strategic level (e.g. frame contracts);
- to develop a method for contract generation - how to go from a general business value model through risk assessment to the generation of contract contents;
- to evaluate evolving standards in the area of e-contracting, such as WS-agreement.
- to create common models that integrate aspects such as trust, business value, rights and policies with contract models.
- to illustrate through scenarios the integration/migration between the proposed six levels of contract-based operational interoperability and the three levels of semantic interoperability (see II.3.3).

I.4.2.3 Non-Functional Aspects

Within the non-functional aspects focus area, one specific area of research, which links the first two of the identified topics of interest, is the model-driven development of runtime support mechanisms for non-functional aspects. The aim is to specify an (abstract) platform model that describes the runtime support mechanisms for NFA in a precise way, and which forms the target for a mapping from “platform-independent” NFA (aspect) models to “platform-specific” runtime support for NFA. There is a need to investigate how the prevailing MDD techniques should be extended to achieve this mapping.

A second specific research area, related to the third topic of interest, is a comparison of the Technical, Formal and Informal (TFI) framework and the InfoSec model for Information

Security, in order to find similarities and dissimilarities. The goal is to investigate how the TFI-model can be applied to an information security model and vice versa. The results of this research will be validated by means of an in-depth case study in the healthcare sector.

I.4.2.4 Digital Rights Management

The working group has identified a set of concrete interoperability issues for further work. Semantic interoperability of DRM systems is among the most important issues, having both organizational and technical implications. In this context the interoperability focus is on content, rights and policies. Content interoperability has to provide a common abstraction providing a way to manage any rights-enabled content, independently of the type of content it represents, independently of the policies that are associated with it and independently of the context it is used in. Rights interoperability has to provide a way to ensure legitimacy of actions and user identification. It also has to ensure that the rights possessed will be globally recognized and understood. Policy interoperability is needed for global understanding and compatibility of the rules protecting content. Decomposing DRM interoperability into these three distinct aspects is necessary to provide the semantic interoperability of DRM systems. Thus the roadmap follows this approach and specific actions will cover each of these aspects, namely:

(i) moving towards a DRM type as a first class citizen,

(ii) managing exceptions in DRM enabled systems,

(iii) creating a policy management framework.

Finally, several relevant application examples are considered from areas of the enterprise environment and mobile agent systems.

I.4.2.5 Business Value

The proposed work for this task group relies heavily on the integration of different techniques and research results from the other areas addressed in this task group. The security aspect is one of the best NFA domains in which to show the usefulness of the proposed work.

More and more institutions want to master the costs and revenues of the ICT part of business critical systems. This can be achieved only through system value analysis and system value management at different abstraction levels and during different steps of the life-cycle. In order to link the results of business model analyses (often resulting in the end-to-end business service value) and business critical architecture analysis (resulting in both organisational architecture and ICT architectures), a value-based and risk-based methodology must be tuned to the current model-driven methods and techniques. This will be done in three different areas:

1. An aspect model and ontology integrating the concept of value must be designed and integrated with the aspects models covered by the different NFA domains.
2. The maturity of NFA support is an important aspect that must be taken into account when considering the value of the organizational and ICT systems.
3. Work will be done on techniques that are aimed specifically at the integration of the value aspects during the negotiation phase of NFA and at the support of the value aspect concerned with NFA during system operation.

I.5 The Next Steps

The discussion of action areas in the preceding section has identified a number of interlocking steps that will carry forward the five main themes. The next stage is to prove the analysis behind this roadmap by detailed examination of a number of these localized steps in specific application areas. This process will give confidence in the work so far and generate evidence on which to base its progressive refinement.

The intended approach in the remaining year of the task group's activities is to subdivide the activities into a number of smaller problem-solving teams, and to test their proposals by the wider peer review offered by publication of the best results as joint papers. Cohesion and architectural consistency will be maintained by presentation and discussion of the work in progress at successive INTEROP workshops. This process will also allow the incremental improvement of the roadmap, so that the main directions are directly available for wider dissemination. Coordination and focus will be provided by the continued emphasis on the five key areas used to structure this document, and on the common cross-cutting issues identified.

The teams are currently forming, and their scope and direction can best be illustrated by the following list of proposals for papers; the resources available are such that only a subset will be carried through, and the involvements given are merely indicative, but the list shows the breadth of the current considerations.

a) Joint paper: "Exploiting trust for privacy preserving integration of data sources" (University Rome, University of Helsinki);

b) Joint paper: "State of the art of trust in e-services" (NKUA, University of Helsinki);

c) Joint paper: "Trust and reputation ontologies and interoperability mechanism: A survey " (University of Helsinki, NKUA);

d) Joint paper "Trust and reputation in e-Contracting" (authors: University of Helsinki, NKUA, e-Contracting group members)

e) Book chapter "Trust and reputation in inter-enterprise computing" to be submitted to "Trust in E-services: Technologies, Practices and Challenges" by Ronggong Song;

f) Potential tutorial on "Data Quality and Trust: How to Converge?", (University of Rome);

g) Joint paper: "Value-model based risk assessment and contract drafting", (KTH, University of Tilburg)

h) Joint paper "Model-driven development of runtime support mechanisms for non-functional aspects" (Telematica Instituut, University of Duisburg-Essen, University of Helsinki);

i) Joint paper "Towards a holistic view of information system security: TFI and InfoSec model comparison" (Luiss "Guido Carli" University, University of Skövde);

j) Joint paper “Social aspects of IS Security: a criminological approach to the analysis of computer incidents” (Luiss “Guido Carli” University, University of Skövde);

k) Joint paper “Permission, Trust, Value and Enforcement between Collaborating Enterprises in the Healthcare Sector” (University of Kent, University of Skövde, KTH, University of Helsinki, University of Geneva, University of Tilburg).

l) Joint paper: “Analysing Interoperability from an Organizational Perspective: Social Dimensions and Technological Support in Bridging Different Communities of Practices (Luiss “Guido Carli” University)

PART II – Detailed Material

II.1 Introduction

This part of the roadmap includes the technical background and justification for the directions presented in part I. The work presented here is the result of a collaborative effort in a number of topic groups within Task Group 7 of the INTEROP Network of Excellence. This Task Group concentrates on the non-functional aspects of the Interoperability problem, and, in particular, on the special interoperability challenges that are related to Trust, Confidence/Security and Policies.

II.1.1 Scoping statement, background and introduction

Non-functional aspects raise several key issues related to Interoperability. These aspects are traditionally introduced for separation of concerns between the main behaviour of an enterprise (functionality) and the supporting technologies and associated management issues that cause alternations to the functional behaviour. Common examples of non-functional aspects include quality of service, security, business value, and so on. These need to be addressed carefully from a business and strategic standpoint. They have a significant impact on corporate governance and compliance, and are, as a result, of a strategic nature within the corporate environment. However, their impact requires us to take a step back and consider their functional implications, in particular by considering how they affect Enterprise Modelling, Ontologies and Architectures & Platforms.

There is currently a lack of knowledge about how these strategic issues affect interoperability, and a need to create approaches and methodologies for their formalization, design, evolution and execution. This becomes all the more significant now that the general scenario of interoperation (e.g., creation of agile, networked enterprises) spans many administrative and legal domains, involving collaborations which are often established in short lived, ad hoc, ways, within loosely coupled environments. Interoperability in this context needs to be studied and factored into designs from the beginning rather than added as an afterthought during integration.

The Roadmap addresses a set of issues of business and strategic interoperability via shared knowledge and stems from the challenges identified during previous, broader work on non-functional aspects within the original Architectures and Platforms focus of the INTEROP network (WP9). These issues cover an initial set of five main topics:

- Trust and Trust Models, Reputation, Privacy.
- e-Contracting, contract knowledge management, business commitment monitoring and fulfilment, and the ontology of contracts;
- Non-Functional Aspects, including generic supporting mechanisms, relating to Security (data/ontology, privacy in data mining, authentication, integrity, confidentiality, non-repudiation, etc.), Information Security, Quality of Service (QoS), Quality Attributes, Performance, Reliability and Availability;
- Digital Rights and Policy Management, Policy Frameworks, Compliance, regulatory environments and corporate governance;

- Business Value, Alignment, Business processes, Risk Management and Asset Management.

In studying these topics, particular attention is given to the Enterprise sector and to industries such as banking and financial services, health care and public administration, and the work is based on the experience and contacts of the task group members. In healthcare, particularly, there is ongoing work on security issues regarding the transfer of patient information between different healthcare providers and the needs and requirements of security in that context.

Concrete objectives that are shared by all the topics covered here include the need to:

- identify and clarify Interoperability issues relevant to the selected topics;
- study the approaches and methodologies for their formalization, covering design, evolution and execution in the context of interoperability;
- identify specific Interoperability Requirements (arising from Architectures and Platforms, Enterprise Modelling and Ontologies).

The topics selected here are the cornerstone of Enterprise Interoperability. They address key issues at the business and strategic level that are currently not otherwise addressed within INTEROP (e.g., business architectures, corporate governance) including shared and agreed security, trust and confidence models, the ability to negotiate consistent policies and contracts, the management of rights, resources and policies, the common semantics and ontologies (e.g. RDD). These issues are important in order to leverage business agility and enable the creation of ad-hoc virtual business processes and Networked Enterprises.

II.1.2 Importance of Organizational Models

One of the conclusions of the work on non-functional aspects in general was that the key to coordinating work on such aspects was to identify a set of precise models of the resources and processes involved in each aspect. If such models are brought into existence, interoperability can be based on the creation of a coordinating framework that allows negotiated agreement between organizations to extend and synchronize them. In this respect the creation of a common model is equivalent to having a shared ontology.

At an implementation level, then, interoperability requires the flexible matching of platforms, based on shared ontologies and policies between the organizations concerned. However, this process must be made dynamic. This requires explicit models of the organizational processes and the lifecycle of the shared models and agreements guiding the moment-by-moment evolution of the platform view that provides interoperability. Each aspect-specific model should inherit from a common core that forms the basis of general management and negotiation mechanisms, so that negotiation can be provided as a common platform mechanism.

II.1.2.1 The Business Level

The agreement by organizations to interoperate may be short term, or it may form the basis of activities over a period of years. What was originally seen as an ad hoc arrangement may evolve to be an ongoing relationship. It is therefore important that the negotiation of agreements is based on stable organizational information, and that this is used to steer infrastructure liaisons that can be updated as necessary to take into account changes in

platforms and in technology specific aspects of the architecture; in model driven development (MDD) terms, the shared models produced should be computationally independent.

This common modelling core needs to include a number of interrelated areas and coordinating mechanisms. It should involve at least:

- A model of the organization and its substructure, and related supporting concepts of naming and identity;
- A trust model dealing with entities, their reputations and their credentials;
- An outline legal framework to support contracts, together with the ability to express basic deontic concepts such as obligation;
- A resource model and associated concepts of value and ownership that can be applied to both tangible and abstract information-based resources.

The target level of abstraction for this modelling must be chosen with care to balance the conflicting requirements of precision and wide applicability. Too little detail will make it difficult to build the necessary agreements, but too much will add to the difficulty and cost of relating the interoperability model to the internal models already established and used within the cooperating organizations. Ideally, the interoperability model should be a common abstraction of the internal models of all the participants, but this ideal cannot in practice be reached without an unacceptable upheaval, and it is necessary to perform some local model transformations that require human initiative, even though to do so reduces the efficiency of the interoperability mechanisms.

Within this framework, mechanisms are needed to increase the scope and level of shared understanding, introducing new services, creating new contracts, or expanding the web of trust. One of the research themes to be pursued is how sufficiently flexible mechanisms can be established to allow organizations to reach agreement, and how they can develop shared strategic policies in a safe and controlled way without threatening any of the organizations involved; in other words, how policy negotiation can be circumscribed to give it a mutually agreed scope.

The aim of this activity is to answer these questions in business terms and to formulate clear targets by which the sufficiency of proposed solutions can be judged.

II.1.2.2 Framework for Relation to Platforms

The organizational models will act as a guide to the establishment of interoperability, but they need to be related to and supported by appropriate platform mechanisms that provide a robust and trusted means of reaching business agreements.

The platform-based mechanisms will typically operate on a shorter timescale and with more concrete objectives than were discussed above in the organizational view. The result will be a dynamically evolving set of ad hoc agreements, constrained by the established inter-organizational strategic policies. This arises from the need to relate to specific platforms and to avoid any changes to the internal processes of the organizations concerned that would be incompatible with the needs for agile and responsive agreements to be formed.

II.1.3 Focus Area Definitions

The earlier work on the state of the art in the support of non-functional aspects concluded that the highest priority for work in NFA was for the creation of a common framework defining the way interoperability depends on the integration and resolution of models and mechanisms supporting a wide range of aspects.

Supporting this, it identified the need for a comprehensive library of aspect metamodels and a rich set of negotiation and integration mechanisms that would allow a commonly applicable interoperability model of the aspects to be constructed dynamically as needed. These were identified as strategic goals that were likely to guide research for a considerable period of time.

This roadmap follows the direction proposed, but concentrates the activity into a small number of focus areas which form the sub-tasks of TG7. These have been selected to cover a range of subjects that balance issues of organizational importance with those that present research challenges in their own right. Thus:

- the item on trust and trust models is of vital importance to practically all organizations, but is also one of the toughest challenges for modellers, because of the need to preserve safety and security targes as the models are elaborated;
- e-Contracts are central to the organizational support objectives of the network, and solutions are also likely to contribute to the notoriously difficult area of formalizing deontic systems;
- the inclusion of other selected NFA areas maintains the breadth of consideration, including a range of quantitative problems and issues from many different analysis and design disciplines;
- the digital rights area and the business value area raise some of the most abstract modelling challenges, involving a full range of organizational policy concerns, while the DRM area also needs to link these considerations with the practical realization of the necessary trusted computing base.

These five areas together, therefore, give us a broad and representative set of activities where, working together, we can hope to achieve results offering both novelty and generality. The remaining sections of this part cover the background to the five areas of work, giving a summary of the issues, current work and directions in each case.

II.2 Trust and Trust Models

II.2.1 Introduction

The introduction of integration of systems or collaborations between independent service components give rise to considerations of trust and distrust between those components, their users, and the environment and context in which those components communicate.

Models and systems developed for supporting trust decisions and activities requiring trust management mechanisms are concerned with a variety of dimensions, as shown in Figure 2. In the figure, layers of interest can be seen as follows.

- Users trust the system or business services they use; these services can be created by a community of networked enterprises, and represented as an agent for the user.
- As part of the ICT system, the applications and users trust the computing facilities and the communication solutions to provide an accurate, unchanged, private service in terms of information exchange and processing.
- The networked enterprises and the distributed computing infrastructures involved consist of agents working on behalf of the business applications, in a collaborative way, and those agents need to trust each other for accurate information, services, unviolated integrity and accurate metainformation about the management of the collaboration.
- The infrastructures for collaboration management must trust that the issuers of credentials, security and privacy policies, identification providers, etc. are trustworthy and follow joint juridical, contractual, and business-oriented regulations and do that in a technically sound manner.

Within those layers, the set of trustors and trustees may also include persons, organizations, infrastructure agents, or application services or information.

The indication of trust depends much on the application areas. The main themes of interest can be captured by the large and overlapping themes of a) inter-enterprise collaborations and partnership, b) exchange of information between users, c) personalization of services, and d) selection and restriction of services used.

For inter-enterprise collaborations, trust information is essential as business collaborations cannot be established or maintained without explicit decisions on trust. Applications in this category tend to be from the fields of electronic commerce and agent marketplaces. In information exchange between users, trust management is needed to be able to determine the credibility or correctness of information exchanged between servers and users or peers, and to protect its authenticity and integrity during the transfer. Network security applications for authentication, and collaborative filtering through recommender systems or in community portals are well represented in this category. In the wide sense, even research engines that rank pages according to how many positive "votes" (e.g. incoming links) they get from the community, are involved in collaborative filtering. The focus is on the trust of the information

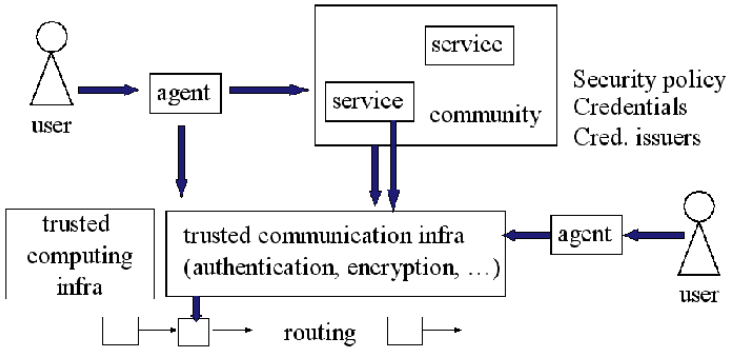

Figure 2: Trust dimensions

recipient has of its source and transfer process.

Trust management can also be used for personalization of services, in order to protect valuable information from external browsing or scarce resources from unimportant use. Some electronic commerce applications and computer network security applications dealing with authorization can be placed in this category.

Finally, trust is an essential element in selection and restriction of services to be used, focusing on the service user's trust in potential providers, using trust for choosing who to transact with. This service can involve e.g. selling goods, providing facilities for printing, performing heavy computations or listing services available in the domain through other providers. Online auction systems, agent marketplaces and some ad hoc, grid and peer-to-peer network applications can be found in this category. Methods for e.g. e-commerce websites to encourage trust in their human users have also been researched in the social sciences.

This part of the roadmap document discusses trust models and management for networked enterprises where both service and information access and composition are involved. The work on models, mechanisms and systems in this area can be categorized into technology, infrastructure, service and community levels. The technology level is closest to the hardware, encompassing e.g. trusted computing components and low-level support for auditing. The infrastructure level connects to fundamental middleware services, covering goals such as determining chains of trust between certificates and managing policies that translate sets of credentials to e.g. local capability tokens. For these layers, see the survey in [GS00]). In contrast to this, this document focuses on the service and community levels, and draws background material from projects like SECURE [C+03], TrustCom [DWR04], iTrust [itr05], TuBE [VRK04], T-SAS [LBLB05] and EigenTrust [KSGM03]. In the service level, trust management wraps around individual applications or services. It affects service personalization and access, but also evolves together with the system, taking into account experience from the trust relationships of the service providers and users. The community level approaches use trust to guide community management, choosing partners according to their estimated trustworthiness and reorganizing e.g. a virtual organization if trust between its members drops too low.

In the following, Section II.2.2 introduces trust-related concepts, and provides a comparison of trust models from the projects introduced on the web site. Section II.2.3 discusses trust management. Trust management refers to collecting the information required to make a trust relationship decision, evaluating the criteria related to the trust relationship, and monitoring and re-evaluating existing trust relationships. In this section, we discuss how system trust can be addressed by providing information and mechanisms for building trusting belief, and leading to trusting behaviour (terms from [MC96]). Section II.2.4 focuses on interoperability issues in trust models, trust management facilities, and in the underlying infrastructure and technology services required to build trust management solutions.

II.2.2 Trust-related concepts and models

Trust and reputation are complex, multifaceted notions, with a range of terms and definitions in the present literature.

From the definitions, we can sieve out an agreement that trust is a quantified belief that the trustee has named qualities. Based on that belief, trust decisions can be taken, leading to a variety of indications. A number of other factors have impact on the trust decision, and these

constitute the context in which the decision is taken. The belief can be computed from a number of explicit trust information elements, or be implicit, embedded in the situation in which the trust decision is taken. There is also a strong requirement for trust to be a dynamic concept, accumulate past experience, and thus provide adaptation to new situations in the networked environment.

Table 1 collects elements for each of the above-mentioned parts of the trust definition from various projects. Surveys containing more references to projects, architectures, models and systems behind this summary table include [V05], [RK05], [C+03], [GS01], [G00], [J96], [BFL96], [MC96], [M94], [TSA03].

Trustee	Trustor	Qualities of the trustee
• person • organization • service process • service step • information source • information element • service provider in respect to a named service • infrastructure agent • credentials/policy issuer	• person • organization • service process • service step • information source • information element • service user in respect to a named service • infrastructure agent • credentials/policy user	• identified behaviour or information content in question • accuracy of information • accuracy of process, or step • appropriateness (correct behav-iour, interpretation for data) • integrity guarantees • identity • conforms to named security/ privacy policy, legislative rules, etc., honesty, truthfulness • competence • dependability: reliability and timeliness

Granularity	Indications	Context
• trust/distrust/uncertainty on result requiring human intervention • trust decision causing either a long-term trust-relationship to be formed or affecting a single transaction only	• using information at face value or with more care • selecting service/ information provider • establishing partnership (contractual state) • restricting information visibility by providing only part of the information • restricting service scope by running only selected service steps	• system components providing audit trails, authorization, identifi-cation, personnel responsibility, reliability/integrity, availability • moral state involving intentions, prejudices/tendencies, beliefs other than trust, knowledge, memory (past experiences and beliefs about other principals, emotions); a particular constituent of this element is the relative weight of the elements of the external context in the evaluation of the trust belief • external context, including o legal system, i.e., the law,

legal principals, contractual agreements

- the social environment, i.e, non-legal principals, rules of communication/etiquette, culture/norms/social expectations
- material environment, including technologies and costs

- risk of the action or use of information
- business value involved, importance of the action, expected benefit from the action
- negative business value or loss in face of mistrust (and denial of cooperation)
- reciprocity

Definitions of trust and reputation are often almost interchangeable. When both concepts are used, trust is generally described as a private measure, while reputation is viewed as a shared or public measure.

The distinction between trust and reputation also underlines the subjectivity of trust decisions, and the use of individual preferences in placing emphasis on different elements of trust information in the decisions. Reputation can be tied both to trustworthiness estimates and expectations of future behaviour, leaving out estimates of appropriateness to the use intended by the trustor.

The trust information (trust and reputation information, context information, other information for the trust decision) has been given various representation formats and metrics. Various numerical ranges and semantic classifications have been used. The trust values need to be interpretable and comparable, but can be created as subjective or objective values, either with transaction-based or opinion-based collection methods. For example, accuracy of information or service can in some cases be measured for forming objective trust measures. However, there are many cases where only human opinions can be collected to give some subjective measure for that trustee.

So far there are no commonly agreed metrics or ontologies for trust or reputation. Several suggestions have been made in the literature (e.g., [ARH00], [DD05], [TD04], [DA04], [CS01]), and some consortia suggestions are under development (e.g., [M04]). The specifications most closely related to trust concerns (P3P, SAML, XACML) are based on XML, thus providing a common syntactical framework without guarantees of conformance between different specifications.

Besides the metrics of trust/reputation and the methods for creating trust values, the way the information is organized and made available is of importance. Trust information can be represented as a global directed multigraph of trust relationships or reputation information

(opinions of trustors about trustees). Such a graph supports the use of global trust functions [ZYI04]. Global trust functions give answers about the comparative trustworthiness of trustees or provide trust-based rankings of service providers. With these graphs it is also natural to support transitivity of trust: if A trust B, and B trusts C, then A trusts C as well.

If transitivity and global trust functions are not considered as key goals, local trust decisions with multiple reputation networks feeding-in information are a natural organization mode. It can be expected that local trust functions would scale better in an environment of autonomous organizations, and also, localization of critical trust information avoids privacy concerns that are associated with global graphs.

Transitivity-related properties in the trust models can be divided into global view phenomena (transitivity in trust graphs) and local view pseudo-transitivity (trust through recommendation). In the global view approaches, a graph represents trust relationships as directed edges between principal nodes [GKRT04]. For the graph, different types of trust propagation methods can be defined, such as direct propagation, co-citation (similar tastes in trusting), transpose trust (trusting also the judgment on trust issues made by trusted peers), and trust coupling. In the local views, no shared global graph is required and each principal keeps a private record of trust relationships. Some of the relationships are direct and formed by local decisions, experience, and knowledge, while others are made by the recommendations from other parties (conditional transitivity, [ARH98]). Recommendations are assertions about the trustworthiness of a third party, and the receiver can make private judgments on the quality of any received recommendations. Trust relationships formed based on recommendations are called indirect [JP05], [ARH98]. Trust on the quality of recommendations and of recommenders is called referral trust [JP05].

The assumption of complete access to information is especially relevant in reputation systems. Some models assume that every principal has the same access to all experience information, and can therefore produce a global view of any other entity's reputation. While this is possible for some applications, typically ones in which all experience information is stored on a centralized reputation server, it is unfeasible for e.g. peer-to-peer systems with limited connectivity or large numbers of nodes, each storing information locally. A global view becomes impossible immediately if principals are allowed to withhold experience information, which is often the case: who can force an independent actor to give an honest opinion or even a fixed-form report without any interpretations?

In the face of limited information, peer-to-peer networks can use localized broadcast requests for experiences and opinions, which are forwarded for maximum coverage, or each peer may broadcast its new information without it being requested, if the amount of traffic and the size of the network are small enough to accommodate it. Applications with centralized servers can store and retrieve information similarly. There is a considerable difference in the vulnerabilities and coverage in implementations accepting items of information from any principal willing to send it when compared to queries for information directed to a selected subgroups of principals.

Issues of transitivity and delegation of trust should be discussed as separate. Delegation of the authority for making trust decisions does actually create a situation where a party decides on trusting other parties the way the addressed agent does. However, the delegation decision is independently made in a situation and can later be withdrawn. In a transitive trust model, the model itself embeds the property. With a non-transitive model with support for delegation, it

is also possible to distinguish between delegation of trust decisions and delegation of the rights for further delegation.

II.2.3 Trust management

Trust information and other elements affecting trust decisions change over time as the context of the trustor changes and the trustee properties either change or become observed. Therefore, trust management facilities include categories of:

- initialization of trust information for a trustee,
- observing or measuring properties of the trustee and accumulating that information as trust or reputation values,
- use of trust information for trust decisions,
- managing trust relationships (contracts) and delegations,
- managing and interpreting the integrity of trust or reputation information.

The trust management facilities depend on infrastructure services that provide secure and trustworthy identification of trustees (or, if anonymity is desired, traceability of the trustee), and secure and private communication.

As an industry driven approach, the Web Services technology family provides a topical framework where an architecture with identification authorities and credential token issuers is presented [GN05]. Furthermore, federation between different authorities is defined [KN03]. Other recommendations in the group provide for dependable service provision and secure messaging between service providers. However, this scheme is less rigorous than is visible in the research arena.

Creation of initial trust/reputation values for trustees can follow a number of methods. Often, the same methods can be used for slowly updating the values as new information is received. The frequently used methods can be classified [ST04], [DA04] as follows:

- Statistical models and tools such as regression analysis, median, mean for estimating the trustworthiness of the trustee. For example, in eBay, the providers receive opinion-based feedback (-1,0,+1) from the requesters. The feedback received by a provider is arithmetically accumulated to estimate the trustworthiness of a provider.
- Social network-based models that follow social relationships between peers when computing trust and reputation values (e.g., [SS01]).
- Probabilistic models that use probability distributions over the set of possible behaviours of the trusted agents and thus represent uncertainty more accurately than the statistical techniques. Works on using the probabilistic estimation techniques are mainly based on the Bayesian [BLB03] and Dempster-Schafer theories.
- Game-theoretic reputation models that encode trust in the equilibria of the repeated game the agents are playing. Thus, for rational players, trustworthy behaviour is enforced. Example systems can be found in [KW82], [FL89], [DR03].

For open networked enterprises we can add methods of assessment and negotiation. Assessment involves an inter-organizational, human driven process to ensure that willingness to collaborate exists, and for this willingness, an appropriate trust model is created.

Negotiations can be partially automated, assuming that agents are given an appropriate set of rules for some straightforward trust decisions and contract establishment. The initialization process may involve creation and exchange of credentials.

Methods that are sensitive to the context and progress of collaboration, and combine direct interaction with peers, witness peer opinions on interactions, and statistical methods have also been developed (e.g. [DCH04]).

Information about the trustee can come either from first-hand experience or from indirect statements. The latter can simply be direct reports of other peers' experience with the trustee, or they can be accumulated values of the peers' general opinion on the trustee. This assumes that the trustee's identifier is either the same as or can be converted to the identifier it uses in the referral providers' systems. The collection and accumulation techniques for indirect statements are the focus of reputation systems research.

For collecting local, first-hand experience, some kind of monitoring is needed. While manual user input and estimates work for some applications, they do not scale well. For service providers with trust-guarded service access, application-level intrusion detection may be of use. Monitoring may be based on specifications of good behaviour, such as duties defined in contractual agreements, or it can be based on a profile of normal behaviour and detect changes from that. Monitoring and accuracy measuring techniques have been surveyed separately for services [V05] and for data [SMB05].

In the common case when indirect statements cannot all be taken at full face value, incorporating them in the local view about a trustee's trustworthiness requires somewhat more complex methods than a corresponding incorporation of first-hand experience does [S04]. A possibility exists for collusion between agents to provide false recommendations, so there is a need for trust evaluation of recommenders, which can lead to circular dependencies between trust and recommendations. The specific collection method used to obtain indirect statements is not without consequence either: for example, gathering statements sent voluntarily from any peers willing to send them may be more vulnerable to liar farming than sending queries to a chosen list of other peers. On another axis, while a centralized storage of statements may ease searches and, assuming it has no bias, make all available information reachable through one point of access, it has other drawbacks when compared to the relative robustness of pure peer-to-peer reputation systems where each peer collects its own, incomplete view with the help of some other peers.

The important trust relationships for networked enterprises comprise those with current collaboration partners and with potential collaboration partners. For potential partners, reputation information is sufficient, as long as it is detailed enough. At present, there is a tendency to require not only information about the image of the enterprise in general, but trustworthiness on specific transactions or types of information. For current collaboration partners, the trust information can be more detailed and associated with commitments to provide certain services under the threat of agreed sanction processes being performed (e.g., [VRK04]).

Trust can be negotiated by exchanging credentials, and the process should preferably be automated. However, some credentials may be sensitive and additional care is needed about when to use them [W03]. Trustbuilder [WSJ00] includes credential access policies in the automated exchange, and the trustee can e.g. aim to provide a minimum set of credentials to fulfil access requirements with the help of a Service-governing policy. If the set of credentials

to present include some that the trustee considers sensitive, the trustee asks the server for its credentials before showing the sensitive credentials. Above, we have assumed that elements (services, information, providers) of the constellation are to be selected so that they are trustworthy. However, we need to consider also the alternative viewpoint: identifying trust and security requirements for a particular environment. There is a need to independently model both the level involving roles and positions and the agents themselves, and solve possible conflicts between the two levels [GMMZ05]. Agents have goals and will execute various tasks in order to satisfy their goals. They can depend on other agents for resources, or for having tasks executed or goals accomplished. They can also own and provide services, delegate permissions or obligations to use or provide them, and trust that the services are used correctly or the obligations fulfilled. Koshutanski and Massacci point out challenges in credential negotiation caused by stateful business processes and the principle of separation of duties [KM05a]. They propose a logical framework and an algorithm for access credential negotiation in the environment of stateful business processes for Web Services. If the credential set provided by the client is not compatible with the server's requirements, the client is directed to revoke excessive credentials from the server and send missing ones.

An essential aspect for trust management between enterprises is the dependability of the services they provide; the service providing platform should be secure and architected according to the requirements discussed in Section II.2.5 for secure computing and communication, as well as on the secure identification and credentials authorities (e.g., [HDA03]). The trust management facilities build on the general security facilities, and provide more support biased towards the business processes and business value and willingness of enterprises for collaboration. This more pragmatic level is often addressed with policy-based, or policy-governed systems.

Well-known policy projects include Ponder [DDLS01] and Sultan [GS01], Delegent [R03], PolicyMaker [BFL96], KeyNote [BFK98], REFEREE [CFL+97], and KAoS [TBJ+03]. Ponder is a policy language and a control system targeted to unite various policy language concepts for access control, and to provide a separation between policies and implementation. The Ponder system analyses conflicts and inconsistencies in the policies, and can provide reports on e.g. what particular actors are allowed to do. Policy types include positive and negative authentication, rights to delegate a task to another actor, obligations and refrain policies. Sultan provides a means to express context-specific trust relationships or recommendations. It can use Ponder statements as conditions on trust or recommending, and Ponder can use Sultan statements as conditions of its own. Delegent is a centralized authorisation server, designed to manage the policies of multiple applications. It implements the Privilege Calculus framework [FS03], which considers positive and negative authorization, refrain as well as override policies, where access should be allowed e.g. in case of emergency but the conditions are not machine encodable. The access must then be authorized or sanctioned after the fact. Constrained delegation of rights is supported. PolicyMaker, KeyNote and REFEREE implement and build on the model where there is separation of authentication from authorization [BFL96] by assigning access privilege certificates, which would then only require a challenge for the certificate holder's private key.

Finally, there is a need to consider the trust information quality itself. Some trust models also internally consider the confidence placed on the input of the decision leading to trust estimation. Confidence estimates are most commonly tied to the view of the trustee: if local experience and external reputation information are scarce, any trustworthiness estimation remains a guess. In theory risk values, for example, could also be developed from experience

and therefore be subjected to confidence, but it is harder to see what exactly is missing from a risk analysis than from trustworthiness estimation.

II.2.4 Interoperability issues of trust

Interoperability issues of trust are strongly dependent on the application area of interest. In the following, areas of interest within the TG7 group are briefly discussed, i.e.,

- Inter-enterprise collaboration and e-Contracting; and
- Information exchange and composition.

Setting up a virtual organization for e-commerce applications or to provide a consolidated service from multiple service suppliers requires negotiation of contracts in such a way that trust is considered as a necessary prerequisite. The contracts will form a basis for policies relating to the entities' rights and duties within the virtual organization and the service level agreements for customers. This must map to policies governing the interactions, which must also adapt as trust changes with experience, risk, or transaction value. Automated techniques and tools to support this do not yet exist.

For e-Contracting, trust decisions can be considered as local functions, while the established contract forms a community in which specific contract-supported trust beliefs are formed. However, for the success of the contract negotiation, an agreed set of trust elements has to become part of the e-Contracts. When trust decisions are local, the requirements for trust interoperability are minimal: the requirements are directed towards the reputation information ontologies and reputation systems themselves. Managing reputation information for e-Contracting may involve composed or federated trust domains. The reputation information should be provided through trusted organizations that manage identities for service providing communities and maintain reputation information for them.

Ontologies provide formal specification of concepts and their interrelationships, an important purpose of which is sharing of knowledge between independent entities. In the context of trust negotiation, ontologies can be used to share information about credentials and their attributes, needed for establishing trust between negotiating parties. Such work is done in [LNO+04] where the use of ontologies is proposed to simplify the tasks of policy specification and administration, and to avoid several information leakage problems in run-time trust management in open systems. It is stated that ontologies describing standard types of negotiations can help to protect sensitive information on behalf of the requester of a resource and of the party providing resources who may want to disclose only information that is relevant to the task at hand. These ontologies contain properties that will describe typical attributes required in the specified negotiation, without specifying any additional constraints.

The contexts of message sender, receiver, and mediating network can have influence on the degree of trust the receiver assigns to a message. In [TD04] ontologies are defined to capture context-sensitive messaging and trust, as well as to provide a basis to propose trust evaluation functions.

For successful business processes, information exchanged, composed and manipulated needs to be trustworthy. Scenarios of interest include virtual districts in e-Business or public administrations in e-Government.

At present, the Web and other loosely coupled environments form an especially interesting environment for peer-to-peer data integration solutions. In such P2P environments, peers interact without previously established mutual agreement and knowledge.

Different methods for measuring and monitoring data quality and the reputation of data element providers have been suggested. Currently the trend is towards a smaller granularity of data collections labelled with trust meta-information. Lack of shared understanding of the metrics for information quality seems to be one of the gaps needing further work.

Management of trust information by the supporting computing and communication infrastructure creates a new level of privacy problem; not only is the information about the activities of a person, organization, agent, etc. potentially to be considered private, but also the accumulated information about the trustworthiness of the entity must be. The privacy issue is a fundamental problem in pervasive systems, which inherently track information such as activity, location, and various other kinds of personal information. In most cases, the pervasive infrastructure is responsible for this tracking (as in cellular phone systems). How can you trust the organizations managing the infrastructure to use this context information responsibly and not pass it on to inappropriate third parties? The same issue applies to any organization trusted to monitor personal or medical information. Using anonymity or pseudonymity to support privacy in pervasive systems has trust implications as well; trust models and mechanisms have to cope with entities with hidden identities.

Interoperability between different kinds of trust decision or reputation management system requires mapping of similar concepts and services between systems. As pointed out in [ST04] there are several trust models that use similar concepts such as conditional transitivity, recommendations or referrals, context-based trust, etc., and the identification of these common concepts could be a starting step towards achieving trust model interoperability. Attaining this interoperability will enable peers with different trust models to interact in a seamless fashion with each other and provide greater application flexibility.

II.3 e-Contracting

II.3.1 Introduction

The Internet allows organizations not merely to share their information and knowledge, but also to integrate their processes and supporting enterprise applications. In previous years, attention has been devoted largely to integrating internal data and processes. However, the advent of intelligent agents and web service technology has leveraged integration of processes beyond the boundaries of organizations. Web services hold the promise to support ad hoc trading collaborations between enterprises by allowing them to be dynamically discovered and combined into aggregated services. At present, however, this promise is still far from reality.

Various researchers have proposed to address the coordination of inter-organizational business processes from a contract perspective. The term “contract” is relevant for two different but related reasons:

- **business**: an inter-organizational business process often represents a business transaction and thus comprises a contract from a legal point of view. This contract contains the legal obligations of the parties involved about some value exchange.

- **technical**: in an inter-organizational business process, we have to deal with the choreography or coordination of private business processes. It makes sense to separate these coordination aspects from the functionality of the applications (web services) involved. The term ”contract” is used metaphorically for the high-level description of the coordination aspects – whether this description has a legal status or not.

It is important to keep these different perspectives in mind, as some research work focuses on the legal/economic aspect only, and other work focuses on the technical aspect only. However, according to many researchers, in the context of interoperable business processes, both aspects should be taken into account and treated in an integrated way. A contract can be defined as an agreement between two or more parties to create mutual business relations, possibly with legal obligations, that governs a certain interaction between these parties. An electronic contract, or e-Contract, is according to [RKKC04] a contract modelled, specified, executed and enabled (controlled and monitored) by a software system.

Contracting may be seen to go through different phases in its life cycle. The most commonly identified phases are:

1. offer/catalogue/selection of partners
2. negotiation
3. signing
4. execution/monitoring
5. contract evaluation

Business contracts have been viewed from different perspectives or divided into different components by various researchers [TT98], [DS97] including:

- Document Centric: Contracts are handled as paper documents or in cases of e-contracting as electronic annotated files (XML documents, ex. TPA (Trading Partner Agreement in ebXML)
- Data Centric: most traditional contract management applications extract the information as data to be merged into other ERP information systems.
- Procedural: a contract defines the choreography in which the parties involved act.
- Communicative: as a set of speech acts wherein the parties declare, permit, prohibit, or promise to carry out certain set of activities in exchange for some consideration.
- Normative: contracts are governed by legislation, regulations and standards specifying pre-described course of actions.

II.3.2 Survey of projects

II.3.2.1 Early projects

In 1980, the contract net protocol (CNP) [S80] [SD81] for decentralised task allocation was one of the most important paradigms developed in distributed artificial intelligence (DAI). CNP's significance lies in the fact that it was the first system to use a negotiation process involving mutual selection.

The notion of electronic contracts for e-business was probably introduced for the first time by Ron Lee [L88]. Lee also wrote several papers on open-edi and mechanisms to establish EDI contracts electronically [L98].

In 1993, the TRACONET (TRAnsportation COoperation NET) system [S93] was presented; the formalisation is based on marginal cost calculations based on local agent criteria. In this way, agents that have very different local criteria, based on their self-interest, can interact to distribute tasks so that the network as a whole functions more effectively. The framework is extended to handle task interactions by clustering tasks into sets to be negotiated over as atomic bargaining items. The TRACONET system was seen as an extension of CNP in commitment strategy.

In 1997, Verharen finished his Ph.D. thesis at Tilburg University in which he developed a agent design framework based on the Language Action Perspective. Contracts represent agreements between agents and are formalized in the CoLa language based on Dynamic Deontic Logic and Petri Nets [V97].

In January 2000, IBM submitted a specification for defining and implementing electronic contracts that are expressed as a TPA (trading-partner agreement). The TPA states the rules of interaction between the parties to the TPA while maintaining complete independence of the internal processes of each party from the other parties [SDN+00]. This was perhaps the first industrial effort dealing with e-contracts.

II.3.2.2 Contractual Agent Societies

Contractual Agent Societies (CAS) are open systems where independently developed agents configure themselves automatically and co-ordinate their behaviour through a set of dynamically negotiated social contracts, which define the shared context of agent interactions, and a system of social control, which is responsible for avoiding, or detecting and resolving exceptions [DK99a] [DK99b] [DK00]

The management of the marketplace consists of a set of homogeneous and mutually trusted agents, including the matchmaker, the socialisation agent, the notary agent and the reputation agent.

- The socialisation service agent negotiates the agent's capabilities and the society's norms.
- The matchmaker agent helps the registered agent to locate another member.
- The notary agent is responsible for storing the contract and resolving potential disputes, and mediates the negotiation.
- The reputation agent stores the history and status (completed, cancelled, breached, etc.) of all contracts formed by members of the marketplace.

In order for (possibly heterogeneous and untrusted) agents to join the marketplace, they would first have to negotiate social contracts with the socialisation agent. The process of socialisation is an enhanced version of the registration process of other agent environments. During a socialisation process, the agent and socialisation services engage in an explicit negotiation concerning the agent's capabilities and the society's norms. As a result of the negotiation between the agent and the society, the social contract is created; it indicates membership of the agent in the society. Once admitted into the marketplace, agents make use

of the matchmaker in order to locate one another. To locate another member of the marketplace, members must send a RFB (Request For Bids) message to the matchmaker, describing the requested service. The matchmaker then broadcasts the request to all potentially eligible members. Interested members may then contact the sender directly by sending it a BID message. After they locate one another, they use exactly the same language they used to interact with the socialisation service agent in order to negotiate a new social contract, which will define their partnership.

Once an acceptable bid has been received, the two parties can start communicating directly, or else negotiate and form a contract through the notary service. The marketplace charges a fee for the formation of contracts. The benefit of forming contracts is that the marketplace then offers a number of "legal" guarantees. If a contract is unilaterally cancelled by one of the parties, the notary service informs the reputation agent. Also, if a contract is breached the notary informs both the reputation agent and the matchmaker. Members responsible for breaching more than N contracts lose their "good standing" with the marketplace. As a consequence, they are banned from further use of the matchmaker.

II.3.2.3 COSMOS

Electronic contracting projects like COSMOS have proposed architectures and frameworks for the automated contracting process. Griffel in [GBW+98] has described the technical foundation for the COSMOS project as based on CORBA and the Business Object Model. They present the Contract Object Model to identify the main component classes of their object model. The COSMOS project identifies the who, what, how, legal parts of any contract. A similar identification is done in the 4Ws approach proposed by Angelov and Grefen [AG03a]. However, in the legal part the approach taken in COSMOS has veered towards a textual document-centric analysis. The actual contract has been modelled as a composition of legal paragraphs containing clauses etc. The primary objective of COSMOS has been to facilitate electronic contracting through all the phases from negotiation using service brokers, and contract drafting using component-based contracts. They have used PAMELA (Petri-net based Activity Management Execution Language) to model the contract execution flow model. This research proposes the use of UML (Unified Modelling Language) as a knowledge representation language and focuses predominantly on contract execution monitoring and workflow deduction using EPC (Event Process Chains).

II.3.2.4 Deontic Logic

While COSMOS has taken a document centric view of the contract, Yao-Hua Tan has dealt in detail with directed obligations, permissions involved in trade contracts in [TT98] from a legal and an action (process) centric view. He has used deontic logic to model the notions of permission, rights and obligations. He aims to resolve ambiguity in interpretations of trade relationships by building formal models for the obligations involved. He has viewed obligations as relationships between two agents. He also introduces the concept of bearer and the counterparty agents who are the two roles of the parties involved in the trade contract. He has modelled several instances of legal obligations and permissions and their legal implications. However, we find that he has not considered the business domain aspect of a legal contract. The relationship between an obligation and its corresponding performance or non-performance has not been taken into account in the obligation model. Also, the remedial option for obligation non-fulfilment has been assumed to be only that of legal action, which is

not always true in the business domain. In another paper [TT02], he has demonstrated the use of event semantics to model contracts and then used prolog to implement the model.

II.3.2.5 Electronic Contracting

In another piece of research on electronic contracting, A. Daskalopulu has analyzed contracts for the purpose of establishing contract performance monitoring in [D97a], [DS97], [D02], [DM01]. She has also promoted the legal centric view of a contract. Her work has been focused around automated contract enforcement and monitoring. She has identified the main issues for contract performance monitoring as (quoted from [D02]):

- To establish what each party is obliged or permitted or prohibited to do at a given point of time.
- To determine whether each party complies with the behaviour stipulated in the agreement.
- Where a party deviates from the prescribed behaviour, to determine what remedial mechanisms are applicable, in order to return the business exchange to its normal course.

Daskalopulu also holds the view that software agent aided electronic contract enforcement and performance monitoring is too restrictive for realistic commercial purposes. Thus she proposes a framework for an artificial controller who forms an opinion based on evidence-based reasoning. In this aspect, Daskalopulu uses Subjective Logic to support her proposal. She has modelled as state diagrams contractual transactions like that for a simple pizza-ordering example illustrated in Figure 3 below, extracted from her publication [DM01].

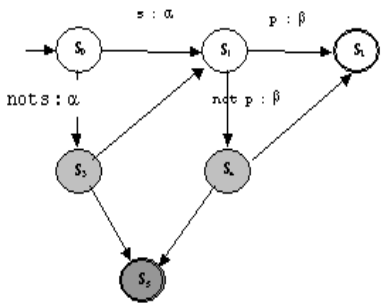

Figure 3: Contractual state

She has associated the events that occur, like the delivery of pizza (S0 to S1), or the pizza not conforming to the order, or the pizza being late, etc. to the obligation status going from obligation satisfactory (S1) to obligation unsatisfactory (S3). In case of exceptions, she proposes a tolerably unacceptable (S3) state, in which the transaction may return to normality, for example if the right pizza is redelivered (S1), or in an intolerably unacceptable (S5) state, when the transactions cannot be recovered, as when the agreements are terminated and litigations started. In [D97a], a combination of modal action logic and deontic action logic has been used to represent the normal, tolerably acceptable and intolerably unacceptable states, making them more distinct.

II.3.2.6 RuleML, SWEETDEAL

Moving on, we find efforts in the current trend for adopting XML as the standard business language for information systems. Grosof in [GLC99] has proposed Courteous Logic Programs as a declarative approach to model the business rules and policies as expressed in contracts. Grosof has further presented an XML based rule representation language RuleML and has also used it with ontologies to produce SweetDeal [GP03], an approach to aid automated creation, evaluation, negotiation and execution of contracts. He has viewed contracts as specifications for processes thereby conforming to the process centric view. Business practice (rules and policies) plays a major role in his approach for handling contracts. He has dealt with two of the domains, business and information technology, but has not ventured into the legal aspects of contracts.

II.3.2.7 Contract Monitoring

The dissertation of Lai Xu at Tilburg University [XJ03] investigates the e-contract and how to check formally whether an enactment indeed fulfils the contract between parties. The e-contract is represented using temporal logic that allows for pro-active monitoring. This means that violations can be found but also reminders can be generated for actions that need to be done in the next step. The checking algorithm has been implemented in a Prolog prototype.

II.3.2.8 Business Contract Language

Contracting using XML based approaches also includes efforts of Goodchild et al[GHM00] who analyzes the fundamental concepts for a business contract and models the contract using UML and XML. However, he has viewed the contract as a document and has placed emphasis on the physical characterization of a contract contents. Milosevic and his team have formulated another business domain and contract integration approach. They propose a framework called the Business Contract Architecture (BCA) [MJPD02] and an associated Business Contract Language (BCL) [LMC+04]. Milosevic defines a contract in [MD02], as ‘a Contract is an agreement governing part of the collective behaviour of a set of objects; it specifies obligations, permissions, and prohibitions of the objects involved, all of which are regarded as constraints on the object’s behaviour in relation to other objects.’

In the same paper, Genetic Software Engineering methods for behaviour trees have been used to identify and model components, states, events, decision and constraints along with causal, logical and temporal dependencies. In the Business Contract Architecture, automation of contract activities like drafting, negotiation, monitoring and enforcement has been considered through the use of software agents. Various tools have been designed to handle each aspect. The Contract Form Editor tool is designed to draft contracts and is predominantly a document centric approach to view contracts as textual documents. A Contract Repository is proposed to store all contract instances and a Contract Notary is aimed to monitor and track negotiations. Finally, a Contract Monitor is envisioned to monitor the contract execution and monitor performance.

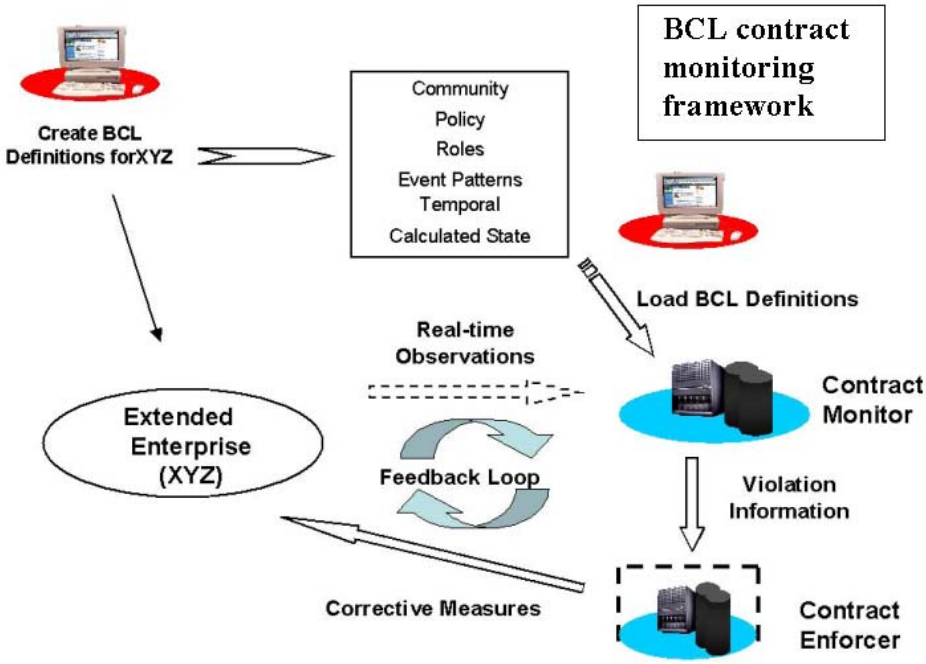

Figure 4: BCA

II.3.2.9 Contract Ontology

Kabilan has envisioned a common ontology framework for capturing implicit and explicit knowledge extracted from the contracting, business and information system domains. A multiple layered framework called Multi Tier Contract Ontology (MTCO) has been proposed [KJ03].

- Upper Level Core Contract Ontology represents a general composition of a contract, which may be applicable across most of the prevalent types of contracts.
- Specific Domain Level Contract Ontology is a collection of various types of contract. Each of the contract type ontology represents a specific contract type like property lease rental, employment contract, and sale of goods amongst others.
- Template Level Contract Ontology, consists of a collection of template like definitions for established or recommended contract models like the International Chamber of Commerce's contract model for International Sale of Goods, European Union's SIMAP online procurement contract models etc.

In this framework, an extended analysis of contract obligations and their fulfilment via the execution of corresponding business processes or activities has been the focus. A state-based analysis of obligation execution has also been considered.

II.3.2.10 Negoisst

Negoisst [SJL03] is a Negotiation Support System for use in e-business developed by Mareike Schoop and her colleagues at RWTH Aachen (currently, Hohenheim). It contains a message exchange module based on the Language Action Perspective that allows the exchange of semi-formal messages. It also contains a document management module. The contract is an electronic document that contains three sections:

1. a detail section - informative part - with some meta-information about the contract, such as dates and contract status;
2. a contract section - behavorial specification - that contains negotiable issues, in particular Action/Deadline items, and the OrderSubject item;
3. a conditions section, including sanctions, or alternative behaviour for specific contingencies in the execution phase.

II.3.2.11 B2B E-Contracting Paradigms

One of the principal researchers in the domain of B2B e-contracting, Angelov, has provided a succinct survey report of contemporary efforts in e-contracting in [AG01]. Angelov and Grefen have defined several paradigms for B2B e-contracting [AG03b]. They define two major types of e-contracting, based on the different levels of automation involved in the contracting process:

1. Shallow E-Contracting, where information systems are used for contracting and the contracts have a digital representation. However, the information technology used does not create new, or modify existing, business processes.
2. Deep E-Contracting; the authors define this type of e-contracting as focusing on all aspects of the contracting process from contract formation, negotiation, signing, execution, performance monitoring, and mainly B2B process handling are included. They again subdivide this category into a number of subtypes (like micro-contracting, just-in-time-contracting, precision-contracting, etc.), based on the type and level of technology used.

Angelov and Grefen have also proposed a framework for representing the requirements as analysed by their e-contracting paradigms called the 4W e-contracting Framework [AG03a]. They define the central concepts for the contract to include Who, Where, What and hoW groups.

- The Who group represents the actors who participate in the contract.
- The Where concept models the context of the contract.
- The What states the exchanged values and their exchange.
- and the hoW models the 'means' for contract establishment.

Angelov and Grefen have focused on e-contracting from the business technology and contracting process perspective. Not much emphasis on the legal commitments and consequences has been placed, like the deontic logic of Tan, or Daskalopulu.

II.3.2.12 EDEE framework

Abrahams et al [AEB02] have proposed an architecture called EDEE (E-commerce application Development and Execution Environment) for modelling business occurrences and contractual terms, policies and, to some extent, the law. EDEE is intended to be able to reason about the interactions between intra-, inter-, and extra-organizational policies. They propose an asynchronous 'Event-Condition-Obligation' style for business process automation. They propose a rule-based approach. They point out several issues with typical synchronous rule-based approaches, including that:

- synchronous rules assume that the agents act only in a predefined manner, upon triggering events, which is in contrast to commercial conditions where a certain amount of leeway is allowed.
- in a synchronous rules approach, although obligations specify deadlines which imply a certain degree of leeway, the synchronised approach invokes business operations immediately rather than at an optimum time within the specified deadline. In the proposed asynchronous rules approach, the authors propose that obligations, events occurrences and execution of actions are brought together asynchronously after consultation with a database, and checking if the obligation has been fulfilled or it still needs to be fulfilled, etc.
- there are other issues concerned with conflict resolution.

II.3.2.13 web-Pilarcos for eCollaboration lifecycle management

The web-Pilarcos architecture and prototypes for B2B middleware [KM05b], [KRMH05], [KMR05] is designed by Lea Kutvonen and her team at the University of Helsinki for inter-enterprise environments to manage dynamic collaborations. The e-Contracting steps involved are a) initiation of the e-Community with a suggestion of the business network model to be used; b) population of the model with service offers in such a way that a set of static interoperability criteria are fulfilled; c) negotiation between the suggested partners; d) community middleware and services setup; e) monitoring of the behaviour of participating business services and breach detection; f) community-level breach recovery. The contract captures aspects both from the business domain and from communication engineering; the categories reflect ideas derived from the ODP reference model.

II.3.3 Identification of specific issues of interoperability

Interoperability can be loosely defined as the ability of enterprise software and applications in different domains to interact. True interoperability is more than connectivity and communication. It includes the possibility that one role performs some service for the other role, and so it assumes that there is a shared understanding of what the meaning of the request is: both the content semantics (activity name, parameters) and the pragmatics (the intended effect, e.g. that the other role executes the request or sends a reject message). This “shared understanding” can be implicit in the code, or be more explicit in an agreed-upon protocol definition, “collaboration agreement” (ebXML), or “contract”. Contract-based interoperability can be defined as: “the ability of applications to interact and work together on the basis of a contract”, where a contract is defined as: “an agreement between two or more roles that governs their interaction in terms of obligations and permissions”. A contract need not be explicit, although this does have certain advantages. In principle, every interaction is contract-

based, as every interaction assumes certain semantics/pragmatics of the communication to be in place, but typically these pragmatics are implicit in the standard protocol that is imposed from the beginning. Several frameworks (ebXML, WS-Coordination) provide the participants with the possibility to define new or extended protocols (agreements) with specifically defined semantics.

In the context of collaborative business development, contract-based interoperability of web services can be divided into six categories [AW05]. Each higher-level category includes functionality of lower levels.

Level 0 indicates that no contract-based interoperability features are supported. Internal functionality of participants of this level allows execution of pre-designated operations; however, only final results (and, sometimes, intermediate status) are externalized.

Level 1. A participant can not only advertise, but also confirm (verify), if requested, its functionality and make a choice of the most appropriate operation (of the same type) to be employed at a run-time.

Level 2. A participant supports one or more transactional protocols. Support of level 2 interoperability indicates transactional interoperability – the capability to be engaged in transactions with some kind of (relaxed) ACID properties.

Level 3. The basic functions are in place that allow participants to make commitments and fulfil them.

Level 4. Participants can monitor a contract. Monitoring a contract assumes that participants are able to understand, execute and verify compliance of other parties' activities to contract clauses. Understanding the contract means the capability to interpret contractual clauses (expressed in some XML-based contract definition language), and support the operations defined in the contract. Execution refers to the internal functionality to fulfil obligations assumed as part of a contract. Finally, monitoring itself refers to the capability to verify other parties' activities against contract clauses and respond with contract-defined corrective actions. Contract monitoring has been the subject of several recent research projects, as indicated above.

Level 5. Participants can not only execute a given contract, but can also adapt a contract by means of negotiation and refinement. This level requires rather developed conversation capabilities and support for obligation-based contract composition. At this level participants are not yet assumed to establish a complete contract from scratch; rather, they should reuse already existing contacts (or templates), compose a contract from other contracts (as in a supply chain scenario) or refine already existing contracts with clauses and parameters relevant to the concrete business scenario.

Level 6 Participants are able not only to refine contract templates, but also to setup a new contract, typically on the basis of explicit goals and preference structures provided by each participant. This functionality implies the use of goal-based negotiations and the ability to extract or compose contractual clauses from sources other then pre-defined templates and samples.

The contract-based interoperability framework can be used to assess current state-of-the-art technology. If we look at web service standards such as BTP and WS-Transaction, we can characterize them as level2. They do provide transactional interoperability by means of which parties can synchronize a certain event, but the business semantics of these synchronized

events (in some cases called “Business Agreements”) are not specified. Therefore, there is also no monitoring of obligations; the only monitoring, if any, concerns the transaction protocol execution. If we look at current agent models dealing with contracts, which are mainly confined to research labs, we can characterize them as level 4 to 5. Level 6 technology doesn’t exist yet. However, contract drafting is a research topic in the area of negotiation support and e-commerce, see e.g. [TT03]. If we look at the ebXML framework, we can observe that in principle, it supports all levels of contract interoperability. However, in practice collaboration profile agreements (CPA) are still composed manually, and the notion of commitment or obligation is not explicit, so ebXML is better characterized as level 2.

In addition to the above mentioned levels of contract based interoperability, we would also like to point out the subtle difference between E-Contracting and Contract Management. While e-contracting deals with the entire process of establishing and executing an *Electronic Contract*, Contract Management can deal more specifically with the execution of a contract – its fulfilment via performance actions. Contract Management could be viewed as a part of e-contracting itself, but it could also involve the management of non-electronic contracts, that is contracts established in the traditional manner, between human counterparts, who sign a paper contract. Nevertheless, the same contract may be transformed into an electronic version and still be processes and executed. Regardless of the technology of *how* a contract is formed, or represented, a contract needs to be aligned with the business processes, be it inter-, intra- or cross-organisational. Thus the semantics of a contract, its implicit and explicit obligations and their implications assume a vital role in the contracting process. Another issue on the operational level would be that contracts are legal documents and thus need to be stored, archived and managed in accordance to governing regulatory frameworks. Also, e-contracting raises the need to establish operational trust between the contracting parties. Especially in cases where unseen partners across the globe negotiate and sign trading partner agreements in ebXML, the question of reliability, credibility, trust and security standards is vital. Another issue is that of digital signatures, rights management and encryption technologies. Digitally signed contracts need to be authenticated, verified and protected against repudiation. Several of the above mentioned issues are indeed the topics of several other sub topics of this task group.

II.3.4 Specific proposals for future work in the INTEROP framework

As seen in the survey of contemporary e-contracting efforts presented above, we see a wide spectrum of related research. Each project has focused on one or more specific goals and perspectives. We see different approaches ranging from rule based (Grosof, Abrahams), deontic logic (Tan), subjective logic (Milosevic) to descriptive logic based approaches (Daskalopulu). We have seen business process oriented (Weigand, Kutvonen) or workflow management oriented (Radha Krishna, Van der Aalst), legal contract monitoring perspectives (Daskalopulu), and shared common contract ontology representation (Kabilan). We have also seen encompassing architectures to cover different phases of contracting (Angelov, Milosevic, Kutvonen).

As has been mentioned in the earlier sections, e-contracting can be said to have different phases or stages in its life cycle. Also, contract based interoperability can be visualised as having six levels (steps), based on the degree of automation adopted. On the other hand, while

increasing the degree of technological (pragmatic) interoperability, we also need to ensure semantic interoperability. Semantic interoperability too can be at different levels:

Level 0: Human-to-Human understanding. Contracts need to be understood by the human counterparts at the different organisations (inter) or departments (intra). The legal document needs to be transparently understood by all parties. This is a primary step to facilitate interoperability between the business processes at a later stage. (CONTRACT ESTABLISHMENT AND REPRESENTATION)

Level 1: Process level Interoperability: Human-to-machine, and machine-to-human understanding. Here the contracts are transformed to electronic versions with the aid of common interfaces or knowledge bases. Policy and other issues to be included via rule based approaches like SWEETDEAL. At this level, though, the contracting organisations may not have tightly coupled B2B transactions; they may nevertheless collaborate on synchronising their respective business processes and activities so that the contract obligations are effectively fulfilled. (CONTRACT OBLIGATION, RULES, POLICY MANAGEMENT)

Level 2: Service Level Interoperability: Here, contract management and contracting is tightly coupled, so that the contract management software is able to track, or monitor the individual contract execution. It is then also able to propose corrections to existing business processes for better contract conformance, or, alternatively, also suggest optimum contract terms to suit existing business process models etc.

Thus a possible line of research would be to integrate existing work/approaches in the context of the identified levels of contract based interoperability not only from pragmatics but also as semantics perspective. In order to do so, the gap analysis would have to be taken into account and missing links to be worked on.

Some specific research objectives that could be taken up in INTEROP are:

- to establish a framework for contract management - including evaluation both of individual contracts and at the strategic level (e.g. frame contracts);
- to develop a method for contract generation - how to go from a general business value model through risk assessment to the generation of contract contents;
- to evaluate evolving standards in the area of e-contracting, such as WS-agreement.

II.3.5 Dependencies and benefits from these actions

E-contracting and contract management *per se* involve issues of trust, security and rights management. The contracting process initiates discussions and negotiations, to establish the parameters for trust and how to build it. The negotiation process is more complex when previously unknown business entities decide to investigate the feasibility of business transactions between them. Trust needs to be developed on different levels: 1. Technologically: how much can one entity trust the message, communication medium, etc chosen? How secure is the transmission? This should involve issues of repudiation as well. 2. Business level: what level of trust is inbuilt in the business organization? It could be based on the company size, its prior reputation and other factors. 3. Legally: contracts are visible tools for building and ensuring trustworthy transactions.

Issues like digital signature verification, security, etc. also have some influence. Thus, this sub task is linked to other subtasks like Trust and DRM.

II.4 Non-functional Aspects: Concepts and General Mechanisms

II.4.1 General overview

Current approaches for the design of interoperable systems have a strong focus on functionality. Non-functional aspects, such as security and Quality of Service, are often added as an "afterthought". However, it is becoming more and more accepted that these aspects should be an integral part of the design process, from the global architectural descriptions to detailed system specifications. In addition, concepts and infrastructure level facilities for managing non-functional aspects should become an integral part of the runtime and service development environments. Note, however, that in some cases it may be debatable whether a certain aspect is functional or non-functional; e.g., in the case of real-time systems, it can be argued that the maximum response time, normally considered a non-functional aspect, forms an essential part of the functional requirements.

II.4.1.1 Overview of non-functional aspects

Many different non-functional aspects can be identified. Below we show a, necessarily incomplete, list of such aspects. We distinguish two classes: non-functional aspects that are usually described in *qualitative* terms, and aspects that are *quantifiable* (although, for some of the aspects that we classify as qualitative, proposals exists to assign quantitative values to them).

- Qualitative
  - **Security**
    - Authentication
    - Authorisation/access control
    - Integrity
    - Confidentiality
    - Non-repudiation
  - Trust
  - '-ilities'
- Quantifiable
  - **Quality of Service (QoS)**
    - **Performance**
    - Reliability
    - Availability

The aspects in boldface are the aspects that we will focus on in this subtask, because they represent best the shared interests of the contributors to the subtask. Also, many of the other aspects are already covered by the other subtasks in this task group. Below, we will explain each of the selected aspects in some more detail.

II.4.1.2 Information security

Information security is concerned with security regarding information assets and the ability to maintain their availability, confidentiality, integrity and accountability. To achieve this, a

number of security measures are needed. These measures are usually described in a layered manner, the two superior levels being *technical security* and *administrative security*.

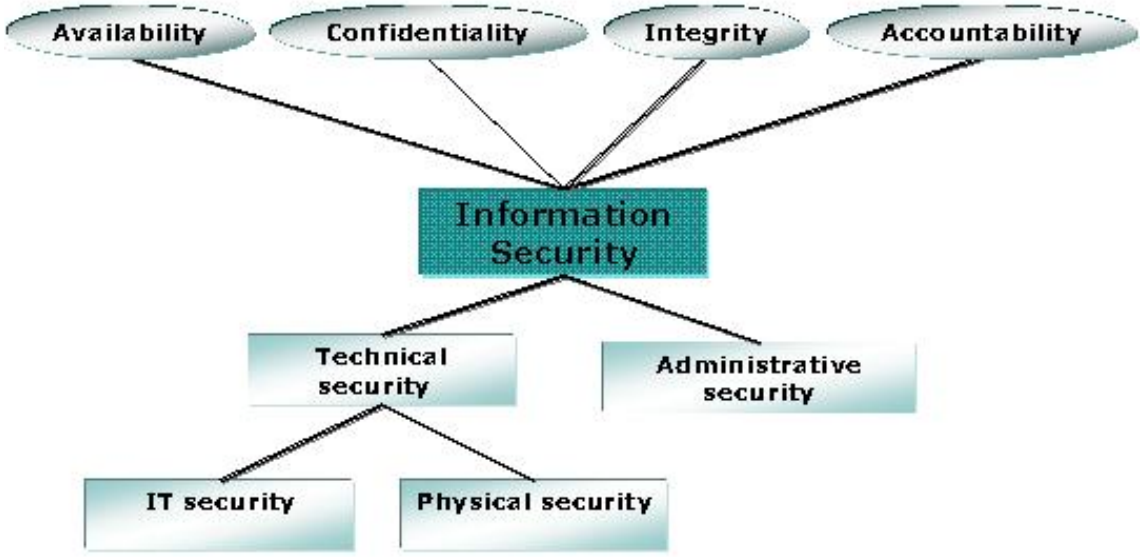

Figure 5: Information Security

Administrative security includes security management, policy management, risk analysis, security strategies, etc., i.e. this part of the overall security architecture is at an organizational level and concerns the business taken as a whole, and takes a stand to what the overall security requirements should be.

Technical security concerns measures to be taken in order to achieve the overall requirements. It is subdivided into *physical security* (physical protection, alarm, etc.) and *IT security* in the form of data and network security.

II.4.1.3 Viewpoints on Architecture Performance

Architectures can be described from different viewpoints, which result in different views on architectural models [IEEE00]. These views are aimed at different *stakeholders* that have an interest in the modelled system. Also for the performance aspects of a system, a number of viewpoints can be discerned, resulting in different (but related) performance measures:

- **User/customer view** (stakeholders: customer; user of an application/system): *response time*, the time between issuing a request and receiving the result; the response time is the sum of the processing time and waiting times (synchronisation losses).
- **Process view** (stakeholders: process owner; operational manager): *completion time*, the time required to complete one instance of a process (possibly involving multiple customers, orders, products etc., as opposed to the response time, which is defined as the time to complete one request).

- **Product view** (stakeholders: product manager; operational manager): *processing time*, the amount of time that actual work is being performed on the realisation of a certain product or result, i.e. the response time without any waiting times. The processing time can be orders of magnitude lower than the response time.
- **System view** (stakeholders: system owner; system manager): *throughput*, the number of transactions or requests that a system completes per time unit.
- **Resource view** (stakeholder: resource manager; capacity planner): *utilisation*, the percentage of the operational time that a resource is busy. On the one hand, the utilisation is a measure for the effectiveness with which a resource is used. On the other hand, a high utilisation can be an indication of the fact that the resource is a potential bottleneck.

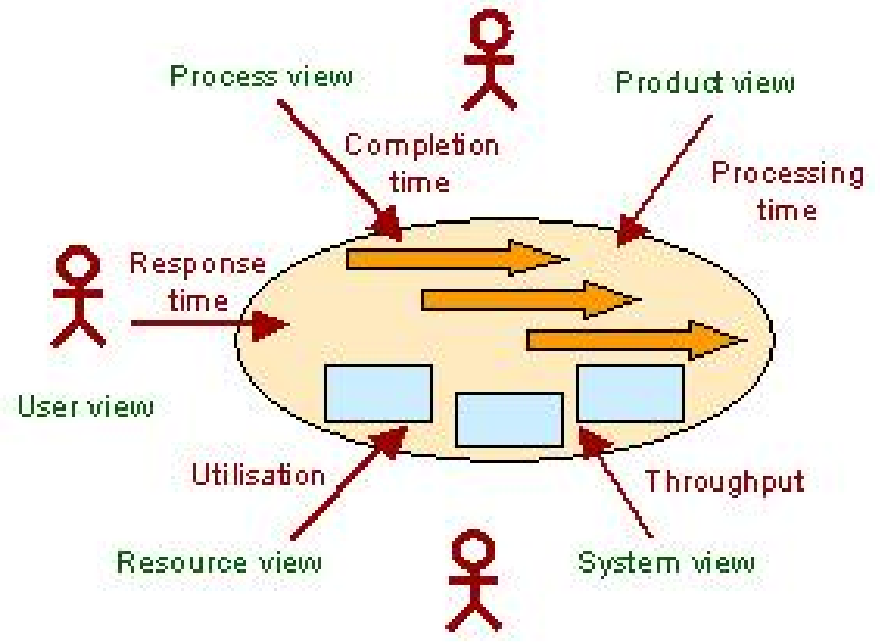

Figure 6: Viewpoints

II.4.1.4 Types of interoperability

In order to study non-functional aspects in relation to interoperability, we need to make clear what types of interoperability we are interested in. E.g., we can distinguish the following types of interoperability:

1. Model interoperability (conceptual): integration of models expressed in different modelling languages, at different abstraction levels, etc.
2. System interoperability: interoperability of actual, implemented systems (where we use the term system in a broad sense: not only technical systems, but also organisational systems)

3. Tool interoperability: the integration of, e.g., modelling, analysis and transformation tools

In model-driven development of systems, model interoperability and tool interoperability are prerequisites for system interoperability. Non-functional aspects play a role in all three types of interoperability: in order to make sure that these aspects are properly addressed in actual systems, they also need to be taken into account in model construction, analysis and transformation.

For all three types of interoperability, we can make a further distinction between *horizontal* interoperability (interoperability within the same abstraction level or functional layer: e.g., business-to-business integration or application interoperability) and *vertical* interoperability (e.g., business-IT alignment).

II.4.2 Identification of specific issues of interoperability

II.4.2.1 Non-functional aspects in MDD

In model-driven development, model transformations play a central role. Vertical model transformations are used to derive, e.g., platform-independent models from computation-independent models and platform-specific models from platform-independent models. Model analysis is another important activity in the system development process.

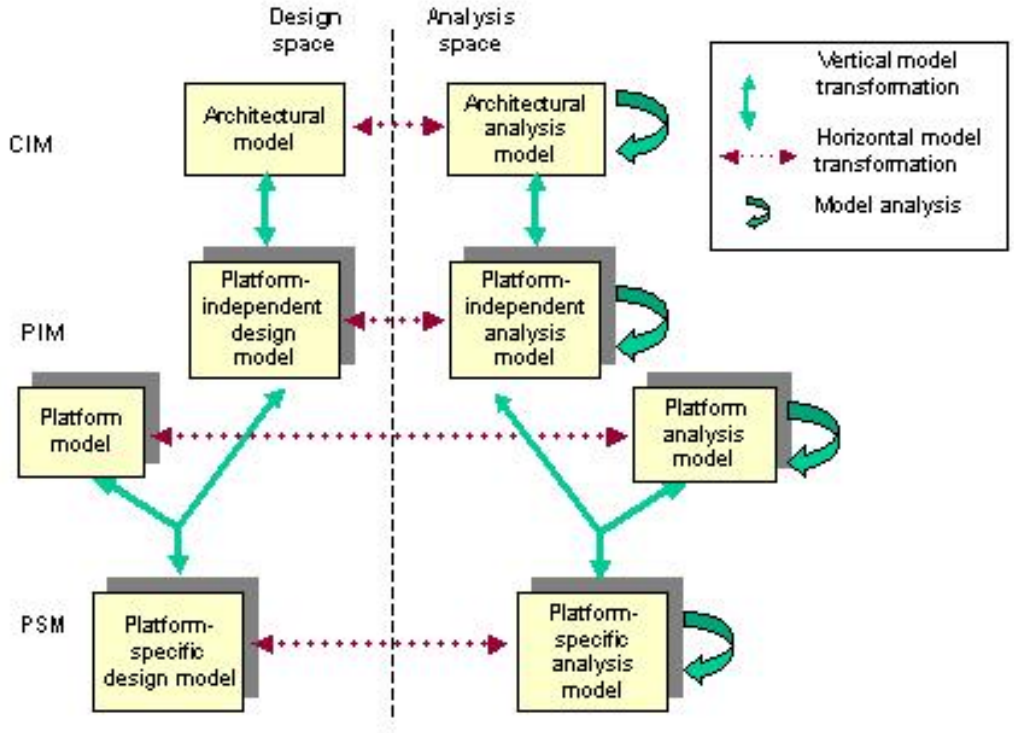

Figure 7: Design space and the analysis space

Analysis can be used in all design stages to check whether the design meets certain (non-functional) requirements or to perform certain optimisations. Analysis generally requires specific analysis models, expressed in a separate formal analysis language. Therefore, we make a distinction between the design space, with design models expressed in design languages such as UML, business process modelling languages or architectural description languages, and the analysis space, with analysis models expressed in a special-purpose analysis language (cf. [SE03]). The derivation of an analysis model from a design model can also be expressed in terms of a (horizontal) model transformation. As Figure 7 shows, there is a strong symmetry between the design space and the analysis space; for any design model, there may be a corresponding analysis model. (See [JILS05] for more details.)

II.4.2.2 Non-functional aspects and integration of software systems

When dealing with integration of software systems, we can distinguish between two different views of non-functional aspects:

1. Each software system that needs to be integrated with one or more others contains its own non-functional aspects, like security, authentication and authorisation. During the process of integration, the different concepts of implementation for these non-functional aspects must be considered and met. This will be quite a challenging task, if the implementation of non-functional aspects is scattered all over the source code of the software systems.
2. The second view of non-functional aspects occurs during the process of integration. For security, for example, it must be guaranteed that data that is exchanged between the integrated software systems is passed correctly, completely and without the possibility of access by a third party from one system to another.

II.4.2.3 Current concepts of integration

Today's integration projects follow three main concepts of integration: A point-to-point (P2P) model establishes a connection between software systems by building one or more individual interface(s) for interoperability. The problems of this model are obvious; as soon as more than a few applications have to be integrated in a company's system landscape, the number of individual interfaces will be too complex to handle, and so further integration projects become more difficult and complex.

Enterprise Resource Planning (ERP)-based integration relies on standard software for Enterprise Application Integration (EAI). Commercial ERP-systems consist of functional modules that provide integration solutions for common business processes. Applications are adapted to these functional modules. Because an ERP-System cannot provide connecting interfaces to every possible software system of a business unit, there is considerable work to be done during the process of adaptation.

A third way of integrating software systems is using middleware products. Message-oriented Middleware (MOM)-based Message Brokers, Application Servers, especially for backend integration of web applications and Web Services for Business-to-Business (B2B) integration are some examples of the middleware-based model. All of these concepts have in common, the property that two or more software systems will be connected to the middleware platform by individual adapters. Adapters convert data and transform messages that are passed between software systems, while the middleware platform implements routing mechanisms between

applications. The concepts of middleware-based integration are not mutually exclusive, but are often used in a way that is complementary.

Here especially, problems occur when implementing an integrative solution. Existing interfaces have to be manipulated or extended or new interfaces have to be written. Changing the implementation of a software system is the most awkward task of an integration process.

II.4.2.4 Integration via AOP

Aspect-oriented programming (AOP) focuses on non-functional aspects in a software system. As soon as such aspects are identified, AOP modularises a task like "authentication and authorisation" in so-called 'aspect classes' to avoid crosscutting concerns. The connection between business logic and aspect classes is established by pointcuts that provide a corresponding assignment. Unfortunately we cannot expect that software systems, that have to be integrated with one another, already provide such a comfortable architecture. The effort of re-implementing a software system for integration purposes using AOP will usually not be taken because of the system’s complexity.

The idea of using AOP for integration purposes is another one: from a software system's point of view the integration with another one can be regarded as a non-functional aspect. So putting the integration logic into one (or more) aspect classes that finally build the connection between the software systems or between a software system and a middleware platform (in this case the aspect takes the role of an adapter), might be another way of planning and implementing an integrative solution. The main advantage of this concept is that the usage of pointcuts might pose a solution to the problem of manipulating existing interfaces. The aspect will be initiated by an event like a method call in one of the software systems. The software system itself will not take notice of the integrating work that is done by the aspect.

A recent idea is to incorporate the idea of AOP in modelling, which also allows for aspect-oriented model transformations [SSR+05]. In this way, the fields of AOP and MDD can be brought closer together.

II.4.2.5 Conclusion

Manipulating and extending existing interfaces is one of the greatest challenges during the process of integration of software systems. AOP has already proven to be a powerful concept as far as the modularization of crosscutting concerns in a software system is concerned. The task for future work is to find out and specify how AOP can be used to reduce the effort to achieve a loose coupling between two or more software systems or to build adapters between software systems and integrating middleware platforms.

II.4.3 Monitoring

Where the above topics are mainly concerned with design-time issues, monitoring of non-functional properties, e.g. QoS properties, is a run-time issue. I.e., interoperability of different (distributed) monitoring solutions is an example of system interoperability rather than model interoperability.

II.4.4 Specific proposals for future work in the INTEROP framework

This task will bring together an overview of existing and new research in this area, including (but not limited to) the following topics described in the subsections below. The partners interested in these topics are indicated.

II.4.4.1 Quality of Service specification and analysis at the architectural level

[Telematica Instituut]

This research is concerned with the question of how to incorporate non-functional aspects, most notably QoS-aspects and security aspects, in (service-oriented) architectures, enterprise models and business process models. Possibly, aspect-oriented modelling can play a role here. Another question is how to analyse quantitative properties of these models. In particular, how can analysis results from detailed design models be integrated at an architectural level [IJ05]?

II.4.4.2 The incorporation of non-functional aspects in MDD

[Telematica Instituut, Univ. Duisburg-Essen, for some overlapping issues: University of Helsinki]

This involves the extension of model transformation techniques to support non-functional aspects (this topic is related to the work in the MoMo TG). It requires an extension of the prevailing MDD paradigm to cover the transformation of families of models for different basic and non-functional aspects to yield a range of platform-specific components and configuration descriptions.

This work should preferably result in a joint research paper by the involved partners.

II.4.4.3 Generic architectures and platform mechanisms for NFA

[Univ. Duisburg-Essen, University of Helsinki]

This involves the investigation of generic architectures and platform mechanisms for the dialogue structures and negotiation processes to support the interoperability features of the complete range of non-functional aspects.

II.4.4.4 Security issues in Service-Oriented Architectures/Web services

[University of Skövde]

This includes general studies of security issues in Web Services, as well as a case study in the healthcare domain. In order to improve the synergy of the research in this subtask, it is useful to see if this work can be linked to the work described in the subsection below.

II.4.4.5 IS security management based on the TFI model

[L.U.I.S.S. "Guido Carli" University]

The definition of a framework to analyse the IS security management system based on the TFI model. Adopting the view of an organisational environment as constituted of the technical, formal and informal (TFI) parts, which are in a state of continuous interaction, this model can be a useful tool when the need to simplify a complex information system arises.

A conceptual analysis about this topic has been performed; a possible next step is the cooperation between partners of the NoE for testing the framework by means of an empiric case study of two or more organisations. An interesting activity could be to perform an in-depth case study describing interoperability issues (in terms of information security) at a technical, formal and informal level when two different organisations begin to cooperate.

II.4.5 Dependencies and benefits from these actions

II.4.5.1 Interrelationship to other subtasks

One of the essential NFA features for inter-enterprise interoperability is trust (and reputation). The trust-related topics are studied in a separate subtask, but the joint areas of work between these subtasks include:

- generic protocols for negotiating about NFA features;
- generic metrics for information (or service/architectural) quality / trustworthiness; trust concepts add to the QoS metrics the aspects about the source and the context of usage;
- business process models extended to address NFA requirements;
- monitoring of the conformance to the agreed NFA conditions.

II.4.5.2 Interrelationship to other taskgroups

The most relevant link we foresee so far is the one with TG3. TG3 is focusing on so-called "model morphisms", covering methods and tools that address the relationships between two or more models (possibly represented in different languages), such as mapping, merging, integration, transformation, fusion, composition and also abstraction and refinement. As we have explained, our view on the integration of design models and analysis models is entirely based on several types of model transformations. Therefore, the results originating from TG3 are of particular importance for this subtask.

II.5 Digital Rights Management

II.5.1 General overview

Digital Rights and Policy Management has become a domain in headlong expansion with many stakes that are far from being just technological issues. They also touch legal aspects as well as business and economic ones [BBGR03] [RTM01]. Information is a strategic resource and as such requires a responsible approach to its management almost to the extent of being paternalistic.

Let us mention as an example some recent cases such as the loss by UPS of a parcel containing the information on 3.9 million clients of a Citigroup company, or the loss of personal data of 600,000 current and former Time Warner employees while in physical transport. These only represent a couple of recent examples of "known" cases of information theft, leakage or disclosure that most companies would have rather not had disclosed. This is probably not new but what has changed in recent years and has "forced" the disclosure of such information is the need for compliance with emerging regulatory frameworks.

Digital Rights and Policy Management is now well established, primarily in two distinct sectors that share the same fundamental underlying technical principles – on the one hand the entertainment and media industry and on the other hand the enterprise sector. This section focuses mainly on the latter.

The objective here is twofold. First it is a plea for raising awareness of the strategic nature of using Digital Rights Management technologies in the corporate environment for Digital Policy Management. To this end we propose a basic guiding framework for corporate policy management. Second, assuming this awareness, we argue that the corporate information systems landscape is on the verge of a profound transformation by which systems will have to factor-in persistent protection, governed usage and managed content – in other words, to become "rights enabled". A key challenge facing the DRM industry that still remains to be tackled is concerned with interoperability issues both at functional and semantic levels. Proprietary incompatible solutions could represent a major legacy and thus a problem for the future. It is thus critical both to address the interoperability issue and to consider the strategic dimension of digital policy management. Interoperability is currently addressed within several other initiatives such as, for example, the Coral Consortium.

II.5.1.1 The Corporate and Enterprise Sector

Nowadays, Enterprise Information systems orchestrate complex processes requiring fine-grained business engineering skills and competencies in order to deliver, in a sound, accurate and cost-effective way, the dynamically evolving services they need. Therefore, this sector is about to witness one of its most profound and significant transformations from the point of view of information management and its organizational and information systems impact.

Currently, information protection still relies mainly on perimeter-based security and access control approaches whether in the local intranet or through a VPN using secure communication channels. However, outside these boundaries it remains a critical issue rarely taken into consideration. This is all the more significant given the broad availability and use of mobile and external storage devices such as USB keys, CD, DVD, PDAs, removable hard drives, etc. All things considered, from the moment information leaves the perimeter or any form of secured extension, and by any means, it is as if it were in clear on the Web. Consequently, the established relationships among parties are based on trust. From a Corporate point of view, this simple form of trust relationship is increasingly becoming insufficient simply from the point of view of the incurred risk and the strategic nature of information.

Policy management nowadays also suffers major gaps. It has now become common to receive an e-mails or electronic document having an upfront statement in bold stating the policy under which it is provided, or a statement saying "CONFIDENTIAL, DO NOT FORWARD UNDER ANY CIRCUMSTANCES, PLEASE". This is wishful thinking with close to zero effect. Forwarding risks, whether intentional or not, are non-negligible. This simple example shows by itself that, while we have definitely passed the point of no return of using electronic mail, there is a point at which organizations are left without means of defence in such situations. Corporate policies still reside mainly in the dusty handbooks often provided to employees upon starting the job. In their most advanced form, these are documented on the corporate intranet basically for reasons of ease of maintenance and update. In most cases, the real corporate policies are split between common sense and on the job experience of employees. It is rare to find companies having instrumented policies and systems enforcing

them, and, to date, none, to the best of our knowledge, have fully-fledged global corporate digital policy management in place. This is a major issue and challenge we have to face in this sector in the coming years.

Facts and Figures

In order to assess some of the key motivations of this domain further, let us consider a few facts, figures and trends. According to the 2001 FBI Crime Survey, information theft has caused the greatest financial damage of all security related problems. A 2002 PriceWaterhouseCoopers report revealed that 32% of the worst security problems were caused by insiders. The Gartner G2 revealed in 2003 that most companies lose intellectual property through employees, whether intentionally or by inadvertence. The META Group estimated in 2004 that, by 2006, about 20% the global 2000 companies would use Digital Rights Management technologies. Etc.

These are a few quotes that are representative of a growing uneasiness in the field of enterprise and corporate security. This uneasiness manifests a fear of facing a security phenomenon that is still so far embryonic: the strategic importance of Information as a resource and asset, as well as the need for mitigation of its associated risk.

Information : A Strategic Resource

Information has become a strategic resource for corporations. It has become critical and increasingly is considered as an asset in digital form: a “digital asset”. The term asset reveals its financial and wealth dimension requiring it to be managed accordingly.

It concerns every corporate functions whether it is HR, legal, accounting and finance, sales, suppliers, customers, budget and planning, production, marketing, design, R&D, competition, analysis and simulations, tax reporting, internal control and compliance; the list goes on and on. None of these functions whatsoever escapes this rule of requiring to be considered as a corporate asset. They all handle more or less sensitive information, be it static or dynamic, requiring various levels of protection and rules governing their use at all time no matter where they reside.

When mentioning dynamic information, we are referring explicitly to all the dynamically generated data created by application portals, ERP systems, databases, line of business applications, etc. often ending up in spreadsheets or files, thus escaping any form of control and protection allowing them to be freely transferred to removable storage devices or worse sent by e-mail to a personal address for further work at home.

II.5.1.2 Regulatory Frameworks, Compliance, Risk and Corporate Governance

The economy and the corporate world have recently been under heavy pressure due to a number of scandals that have raised major concerns for investors and markets. It is in this context that several regulatory frameworks have emerged defining principles of practices, responsibilities (now under the criminal law) as well as the duties of publicly traded companies.

Among the most striking examples was probably the Sarbanes–Oxley Act governing the integrity of financial and accounting data. Another example in the banking industry is the Basel II agreement, which requires banks to comply, by 2007, to instructions to minimize the level of their reserves as far as possible.

By now, there are many such regulatory frameworks either sector based, or categorized by type of risk, etc. These issues now have a direct impact on corporate governance in the sense that compliance is not only mandatory and bounded in time, but must also be audited on a regular basis. The cost of not complying is crippling and may even lead to severe penalties, fines and jail or may even stop the business with disastrous consequences on reputation and image. DRM technologies can, up to a certain point, help in managing these issues and thus mitigate such risks.

Among the most widely known regulatory frameworks that were or are still on the compliance agenda, we find: (classified by activity)

- Financial services
  - Graham-Leach-Bliley (1999) Title V – confidentiality of customer banking data
  - Sarbanes-Oxley (2002) – integrity of financial and accounting data
  - NASD 2711 (2002) – relation between research analysts and investment banks
  - Basel II (2007) – level of reserves based on operational risks
- Health
  - HIPAA (1996) – confidentiality of patient records
  - FDA 21 CFR Part 11 (1997) – data integrity of drug clinical studies
- Other
  - California SB 1386 (2003) – confidentiality of personal data
  - ISO 17799 (2000-2) – best practices for information security

Etc.

It is noteworthy to mention that the compliance issue is a sustainable problem that is here to stay, having a recurring audit activity in order to prove compliance. It is therefore vital for corporations to place this issue high on the agenda not only from specific risk mitigation point of views but also and more importantly at the strategic level of corporate governance. This requires a consistent approach that is global to the enterprise, involving everyone at all levels, as well as defining the right management dashboards for its continuous monitoring. Thus, Digital Policy Management becomes a strategic project under the supervision and responsibility of the top management. It will be only at this price that companies will be able to cope seamlessly with such issues in a cost effective way, not only the evolution of the existing regulatory frameworks but also the certainty of the emergence of the future ones we cannot anticipate.

II.5.1.3 DRM in the Corporate and Enterprise Sector

DRM technology represents the technical means to manage digital assets and define the rules governing their use in a persistently protected way. It relies on the following basic principles common to all sectors where DRM is used:

- Superdistribution [MK90], [MT87], [C94] [C96];
- Persistent protection,

- Definition and expression of rules governing usage and access to digital assets using rights expression languages [S96]],
- Direct or indirect association of these rules to the digital asset.

What can DRM do – and not do – in the Corporate Environment

DRM technology can address and help solve a number of issues that are becoming increasingly critical in the corporate environment. In particular, it represents a solution for the digital management of rights and policies governing content usage as well as the related processes and electronic services. Most common examples are among the following:

- Enables a responsible management and use of digital assets within and outside the corporate perimeter
- Assists in managing classifications (e.g. company confidential, board of directors, projects, etc.)
- Helps instrument compliance management with respect to regulatory frameworks and corporate policies at large (e.g. Sarbanes-Oxley, HIPAA, NASD 2711, etc.)
- Provides a basis for managing retention policies (e.g. e-mails, documents, etc.)
- Provides the means to manage issues facing traceability, monitoring, tracking, usage metering, audit trails, etc.
- Provides a centralized management of revocation and granting rights (e.g. to a new employee, when an employee leaves, etc.).

However, DRM technology does not and never will provide total “military grade” security. The issue is to find the right balance between security and a commercially viable risk. Or, in other words, security stops where the marginal cost of implementing it is disproportionate to the risk one is trying to mitigate. Moreover, technology cannot provide any protection against analogue attacks like reading information over the phone, taking a picture or hand copying. Such cases are however clear and leave no doubts about the malicious intentions, thus allowing legal or disciplinary measures to be taken.

Digital Rights Management: a Help rather than a Constraint

Let us mention here that it is not a question of adopting a paranoid attitude aiming at the total and absolute control of everything – becoming a “big brother”. Rather, it is a responsible and aware attitude and clear general policy with respect to information management representing one of its most invaluable assets and intellectual property.

Given such a context, DRM technologies can provide a more pleasant and safe work environment substantially reducing numerous risks of unintentional errors. It represents a help by providing potential risk detection and mitigation.

Let us consider a particularly striking example to illustrate this. It is now common to work on several projects involving many people and partners. Moreover, it is also not uncommon for an individual to be allocated to different projects at the same time. E-mail remains a wide-spread and heavily used tool for communication and coordination among the project members. Now, how many times do we diligently and carefully check the recipient list when doing a “reply all”? The most frequent and honest answer is “almost never”. However, it is also possible that some people leaving for a few days might decide to use another more

convenient personal address to keep in touch with the project. Now consider one of these persons being fired with immediate effect while away.

Well, in such a situation, if no one pays attention, this person will continue to receive e-mails on his personal address until someone realizes it, if ever. Thus he gains access to information he is no longer entitled to receive and he could easily disclose it to the competition or the media. Moreover, if this person still holds work related data on mobile or removable devices he will still be able to access it freely.

This is just one among many information risk situations, for which DRM technologies can provide significant help in applying and verifying dynamically corporate policies applicable to specific situations. Moreover, by applying those policies consistently to work documents, an employee leaving would immediately trigger the revocation of his rights in a centralized way, thus preventing further access to any documents held, provided the policy required some form of on-line license acquisition.

II.5.1.4 A Framework for Corporate Policy Management

We propose a general framework for studying, analyzing and defining corporate policy management aiming towards its partial digital instrumentation. Our starting point is a basic layered architecture commonly found in the enterprise by using which security issues are categorized into infrastructure, application and content. These three layers traditionally fall under the responsibility of IT and IS, involving the Chief Technical Officer (CTO), Chief Information Officer (CIO) and Chief Security Officer (CSO).

We then introduce another layer for Corporate Policy Management, coming under the responsibility of the top management including Chief Executive Officer (CEO), Chief Financial Officer (CFO), Chief Compliance Officer CCO and Chief Operating Officer (COO). It should be noted that the compliance officer (CCO) has moved from traditional “internal controls” to a top management position and responsibility, mainly in the light of compliance issues. This layer is strategic and focuses mainly on corporate governance. In the scope of corporate policy management, we identified three main sources of input in two distinct categories. The first category is internal and deals with internal corporate rules and policies. The second category is external and has two sources – the business practices commonly applicable for the activity sector and the legal and regulatory frameworks the company must comply with. Now, across these four layers, the three technology ones and the strategic one, runs a recurring audit activity to monitor and assess compliance. Traditionally undertaken by external auditors, it is also the case that such activities are fundamental for those inside the enterprise for corporate governance purposes using management dashboards and indicators. Figure 8 illustrates this general framework for corporate policy management.

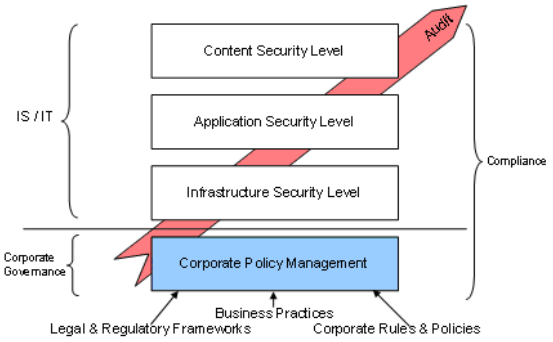

Figure 8: General framework for corporate policy management

Such a framework provides the means to analyze policies in order to determine the ones that can be partially or fully digitally instrumented by technologies such as DRM at the IT and IS level. It should be noted that all policies definitely cannot map to technical solutions. A good example of this would be the notion on "intention" when accessing a report, for example, within NASD 2711. Intentions will hopefully remain hard to calculate in the future. Nevertheless, part of the corporate policy management will be instrumented and the remainder will stay under the control of traditional measures. The instrumented part will provide the means to answer questions such as: who, what, when where, traces, delegations, etc. Figure 9 positions corporate policy management with respect to its sources and its potential digital instrumentation using Digital Rights and Policy Management technologies.

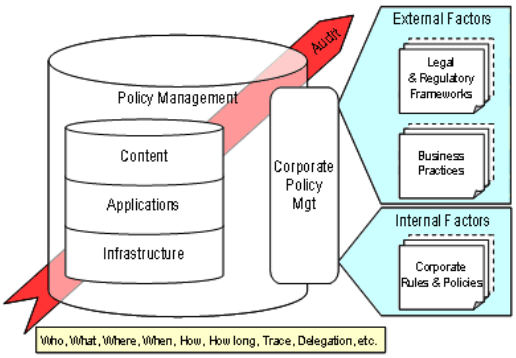

Figure 9: Positioning of Corporate Policy Management

II.5.2 Identification of specific issues of interoperability

II.5.2.1 Towards DRM Semantic interoperability

Nowadays, it is acknowledged that one of the main issues the Digital Rights Management industry is facing is interoperability. Recent standardization efforts have led to the creation of

ISO standards such as MPEG-REL [ISO04a], and MPEG-RDD [ISO04b]. Other efforts towards DRM interoperability are being considered by groups such as the Open Digital Rights Language (ODRL) Initiative [I02], the Open Mobile Alliance (OMA) [OMA04] or the Coral Consortium [Cor2004]. Recently, the IFPI announced DRM interoperability as being its top priority.

Although technical solutions ensuring DRM content interoperability are becoming available, it is still clear that semantic interoperability of DRM systems is not available at all. Some efforts are being made to provide such semantic interoperability, such as MPEG-RDD [ISO04b], but they concentrate on a particular field, namely multimedia. Moreover, apart from technical issues, many other aspects of DRM interoperability issue are appearing. These are induced by economic stakes and the enterprise environment and they also have to be considered.

II.5.2.2 Organisational Stakes

Today's enterprises are an integration of technologies and views. In the near future existing Information Systems, ERPs, KMS, Process Modelling, etc. will have to integrate DRM solutions and usage rights for their content. This raises the following problem: currently there is a lack of suitable abstractions to handle DRM in a truly global, interoperable, way. Enterprise DRM must deal with issues involving multiplicity and heterogeneous contexts.

DRM interoperability is becoming a society-wide issue where we need to know how to protect assets, integrate multiple viewpoints and resources, and communicate with partners. It requires a common ground of understanding and a communication base enabling semantically agreed DRM. This demands a DRM abstraction that provides a uniform way to manage and understand DRM-enabled resources and to allow their integration into the enterprise environment. Semantic interoperability in this context is mandatory as the exchange of resources among partners and communication of them are central to the enterprise context.

II.5.2.3 Technical Stakes

We consider the technical issue of DRM interoperability as being threefold.

First, content interoperability has to provide a common abstraction providing a way to manage any rights-enabled content, independently of the type of content it represents, independently of the policies that are associated with it and independently of the context it is used in. Then rights interoperability has to provide a way to ensure legitimacy of actions and user identification. It also has to ensure that the rights possessed will be globally recognized and understood. Finally policy interoperability is needed for there to be a global understanding and compatibility of the rules protecting content.

Decomposing the DRM interoperability issue into three such distinct aspects is necessary in order to provide the semantic interoperability of DRM systems we want. Thus the roadmap will follow this model and the specific actions taken in this topic will cover each of these aspects.

II.5.3 Specific proposals for future work in the INTEROP framework

II.5.3.1 DRM as a First Class Citizen

DRM and Type Theory

Type theory and DRM interoperability seem to be closely related. The following two quotes were taken from programming literature, but they both apply to the content interoperability issue. In [CW85], authors state that the major purpose of types is "to avoid embarrassing questions about representations and to forbid situations where these questions might come up [...] types impose constraints which help to enforce correctness." This is a goal shared with interoperability, as fully interoperable systems will never have to face such situations. Specifications and standards also enforce correctness. Further, [P02] argues that a type system "is a syntactic method for enforcing levels of abstraction.".

It is clear that the DRM field needs abstractions to manipulate rights-enabled content. A type's properties such as data abstraction, independence, a message-passing paradigm and inheritance [N86] are particularly interesting in this context as they provide both encapsulation and abstraction. Based on such properties, we propose the definition of a DRM Type that can be used for DRM content interoperability. The goal of such a Type is to be the least common denominator of all kinds of rights-enabled content while also being extensible.

Towards a DRM Type

A DRM Type is a common abstraction defining the envelope of rights-enabled content. Similar to other types, it defines a state and provides operations shared by all rights-enabled content. An example of such an operation is a primitive for adding and retrieving a set of rights possessed by the content. These can be required if the content is a composition of other rights-enabled content. Another example of a useful operation could be a primitive for retrieving the actual DRM system able to handle this content. Further, each DRM Type possesses a set of policies governing each rights-enabled content use. The combination of this information thus defines what rights-enabled content is by describing its state, its interface, the policies governing its use and the rights it possesses.

This abstraction thus provides a DRM First Class Citizen that can be detected, understood as being rights-enabled content and handled independently of the nature of the underlying DRM system. This work proposal therefore covers the content interoperability issue presented in the previous section.

Providing a DRM type need a number of issues to be considered. For instance, the presence of a sub-typing relation raises a debate about what are substitutable sets of policies in order to be able to compare types. These questions are directly related to the policy interoperability issue and will need investigation in another part of the roadmap.

II.5.3.2 Credential Based Approach to Managing DRM Exceptions

DRM Exceptions

While having an initial basic level of interoperability among the currently incompatible systems is a critical issue and an enabling factor for the broad endorsement and deployment of DRM based systems, whether in the entertainment or enterprise sector, there still remains a hard problem to be addressed. How do DRM enabled systems manage or otherwise deal with

so-called exceptions? In order to further emphasize this critical issue, let us cite the Copyright Balance principles that should underline public policy regarding DRM as recently outlined by E. Felten in a column in CACM [F03]: "Since lawful use, including fair use, of copyrighted works is in the public interest, a user wishing to make lawful use of copyrighted material should not be prevented from doing so by any DRM system.". This sound principle is exactly at the forefront of this work making the case for such Exception Provisioning in DRM enabled systems.

In a global DRM enabled information market, and provided there is a need for governed content usage (not all content requires governed usage), we assume all digital assets to be persistently protected. We also assume that the content follows the superdistribution model where the rules that govern its usage are either directly and cryptographically attached to the content or can be dynamically acquired on-line. In both cases, it is reasonable to postulate that rights holders cannot anticipate all usage situations within the set of rules, and hence are definitely not in a position to anticipate most exceptional situations where some rights should be waived while still maintaining a given level of persistent protection and governed usage. This is especially true considering a global worldwide market still having complex, often contradictory national and international regulations and legal frameworks. Even if these issues were solved from a legal standpoint, there would remain a tremendous technical overhead in accounting for exceptions and waivers beforehand. Imagine a picture of 100 kilobytes requiring a 1 Mbyte policy. This also becomes critical when considering mobile devices such as PDAs, cell phones, sensors, etc., which have only limited resources.

A Credential based Approach

We propose an interesting alternative approach – a credential based approach by which a DRM module would provide a hook to evaluate locally held credentials that could have precedence over the attached rules and be traceable (i.e. auditable). The process could be rather straightforward as it would be comparable to the existing verification of locally held licenses in the user's license-store. For example, let us imagine that blind and visually impaired users are provided with such a credential due to their disability. Or an academic holds a credential, delivered by the university, showing his affiliation and status. Such credentials would be stored on the user's computer (e.g. in a credential store) and made available to the DRM module (enforcement point) when evaluating rights at runtime.

To be efficient and secure, the credential-based approach implies that the throwing of an exception by credentials must be detected and correctly interpreted. In this context, credentials interoperability is mandatory because the credentials certifying a situation leading to an exception can be emitted by any entity. This will have to be ensured by any solution to this problem, making it part of the rights interoperability issue.

II.5.3.3 Policy Managed Framework

The main idea is to be able to define a policy managed framework based on existing DRM approaches and technologies when possible. The goal of this framework is to support two-level security while providing interoperability. The framework will have to manipulate securely policies generated from models reflecting the decisions taken at a strategic level, interpret them and then dynamically and securely apply them on the application level.

The combination of DRM with policies provides a secure mean of embedding static rules in code in order to control its run-time behaviour. Depending on the situations encountered as

well as social interactions, the framework will be able to trigger different code parts securely as defined in the policies with the assurance that the forecast behaviour will not be threatened. Further, the framework will allow more flexibility and more reactivity to the changes in strategic security policy as the policies can be regenerated and then changed on the fly, ensuring that applications behaviour will always reflect strategic concerns.

In the context, of such a framework, interoperability both of policies and of underlying DRM technologies is required. The framework needs to be able to interpret securely a large range of situations through policies in order to apply them efficiently. This topic thus covers the last of the three aspects needed to provide semantic interoperability, i.e., interoperability of policies.

II.5.3.4 Applications

There follow some particularly relevant application examples of these actions in the scope of INTEROP.

DRM enabled Mobile Agents

The policy-managed framework can be combined efficiently with the mobile agent paradigm, to enable the creation of powerful secured mobile applications. Such resulting DRM-enabled mobile agents would be able to embed statically defined policies defining the way they have to behave. The DRM capability of the framework ensures that the code will be executed as defined in the policies, and that mobile agents will be piloted securely.

DRM enabled mobile agents can, for instance, be combined with e-contracting capabilities. Policies can be used to define how e-contracts have to be built and then to define how they have to be executed. The behaviour of mobile agents and the dynamic creation of secured e-contracts will be piloted through policies obtained from the strategic level. During their lifetime, agents will build e-contracts resulting from the application of embedded policies to the social interactions of the agents. Once created, these e-contracts will be made-up of a combination of different policies indicating what code has to be executed in order to fulfil the generated contract. In this context, policies describe how contracts have to be built and then what other policies have to be used to define how the contracts have to be executed.

On the technical level, the persistent protection provided by DRM will ensure that the e-contracts are built according to the contract creation policies, and also that their execution conforms to the contract execution policies. DRM will also provide accountability and traceability of the whole process of creation and execution of e-contracts.

II.5.4 Dependencies and benefits from these actions

II.5.4.1 DRM Abstraction for the Enterprise environment

A DRM First Class citizen provides an abstraction of DRM content and defines common properties and features that all DRM content have to provide. Among other properties, a DRM type provides extensibility, reusability, comparability and safety, polymorphism and composability. All these features can be defined as the basis for DRM content interoperability, but they are also the reason that have made typing useful in the programming and modelling fields.

Thus in addition to content interoperability, DRM types can enable the use of useful tools and methods provided by the object-oriented world. To name only a few of them, modelling tools could be used to structure DRM solutions easily; design patterns can provide elegant reusable

solutions to recurring design problems. They can also control and shape the way DRM systems communicate with DRM content. For instance, monitoring could be done through the Observer Pattern and maintenance of content ensured through Visitors. Further, analysis tools can help trace information, locate potential issues, estimate the scope and impact of policy modifications or insertion, or detect potential side effects. Finally, as a last example, refactoring tools could enable disciplined DRM type restructuring, altering their internal structure without modifying their external behaviour. Refactoring tools could also help add new features or solve identified issues.

Such organizational features are important for large-scale and efficient enterprise DRM adoption. A DRM type may be a solution to take advantage of them, and thus integrate rights enabled content smoothly with existing Information Systems.

II.6 Business Value

II.6.1 General overview

We first describe the general context of our work which is mainly concerned with a better handling of security in information systems through an improved risk-based management approach based on an improved understanding of the required interoperability needed between the business of the enterprise and the architecture of its underlying information system (IS). The overall approach is summarized in the following picture:

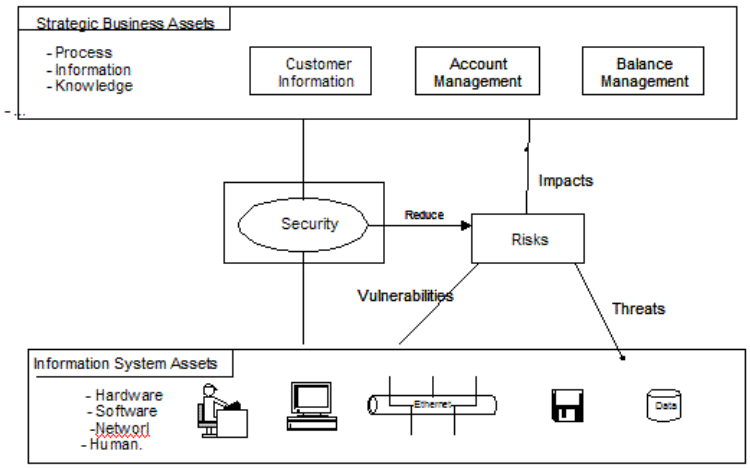

Figure 10: Overall approach

From this figure one can identify the main components of a risk-based management approach:

- Business Assets are anything that has economic value to the organization and that is central in the realization of its business objectives. The protection of these assets is essential for the survival of the organization.

- Within organizations, business assets management relies heavily on information systems. Information System Assets (including IT resources) are any components that are part of IT systems and of their operating environment. In most cases IS assets are the mirror of business assets.

- Security is the central property expected from the installed information systems. It defines different qualities expected from the IS. Besides the pure security aspects (like confidentiality of data), it also encompasses aspects like reliability, performance, resilience, etc.

- Risk management is the essential equation to be kept in mind when handling the different security qualities. For each IS asset, one has to ask questions about its vulnerabilities, the existence of potential threads capable of exploiting these vulnerabilities and the impact of this exploitation on the running business.

Today there is a huge and increasing demand for methodologies and supporting tools allowing the management of IT security risks. This demand is mostly pushed by new legislations and regulations applicable to different sectors and enforcing them to demonstrate how to manage their risk (including IT risks). As an example, we can quote the new Basel II regulation that, starting 2006, will impose on all the actors of the financial sector a requirement to demonstrate how they manage their risks.

A number of commercial methods are now available in the market (BSI, CRAMM, EBIOS, etc). However, they have a number of weaknesses that result from a lack of well-defined concepts, detailed analysis and a more rigorous, analytical and systematic approach. Some of these elements are related to:

- A better characterization and understanding of the business assets. What is the economic value of an asset, how are assets organized in terms of business processes, how better to represent them in a more rigorous way through models (enterprise modelling)?

- A better characterization and understanding of IS assets. What are the components of an IS architecture, what are the components of software architectures (both at a logical and a physical level)? How to represent them through adequate models (like MDA), how to associate to such components security properties and characterizing threads related to them?

- A better classification and handling of security qualities. Can we rely on a taxonomy of typical security qualities (beyond the classical ‘CIA’ taxonomy)? How to relate security qualities to the business assets in a systematic way? How to relate security qualities to properties of architectures (at the IS and software levels)?

- A global interoperability framework. How to manage the traceability required between risks management decisions and all the information collected above?

In the next three paragraphs we further detail the three first items. Then in the next section we handle the last bullet, which is clearly related to the central interoperability problem.

II.6.1.1 Business Assets

In traditional security management approaches business assets are defined as all the information and the processes that need to be secured. However, very little is said about how to identify systematically the business assets and also how to rank these different assets according to their economic value. When answering these two questions, we think it necessary to investigate inputs coming from the business process and business value fields.

Business process

Different enterprises modelling approaches (UEML, BPML, etc) allow us to express the different business activities run in an enterprise, the business actors performing these activities, information flowing between these activities, and also the nature of the information itself. Most of these approaches are supported by a meta-model associated with the notation. The different artefacts of this meta-model need to be reviewed to see which ones correspond with business assets. For example, a business actor with a number of skills can be considered as a business asset of the organization. The same is true for a process, which, if it is disrupted, can endanger the organization, etc.

Business value

At some stage of the security management process it is also important to be able to rank the different business assets because, depending on their degree of importance, different security measures (with different costs) can be envisaged. Work related to the business value of an asset can be found in particular in TG5 where the concept of economic value is embedded in the concept of process model.

The Business Model is an important component of the Business Strategy that the works of Gordijn, Osterwalder and Pigneur have studied more specifically [OGP05]. The Business Model can be used to describe the relationship between the Business Strategy and the Business [OP04]. Central to the business model is the concept of economic value.

In the current work of the TG5 task group, an important part of the Business Model Engineering is the engineering of the Business Value. The model of e^3-Value [GA01] shows how to engineer value creation with a net of value exchanges. The works of Gordijn explains how to analyse this net, and how to compute the resulting value of the net. With this view, the business processes have to give support to the business value net. However, the business value net is almost always built involving different organizations. This implies that the interoperability aspects of the business process engineering is very important in order to give adequate support for the value net.

Understanding the relation between the business process model and business model is therefore essential in our roadmap.

II.6.1.2 Information systems and computer-based assets management

Similarly to business assets we need also to come up with a taxonomy of assets manipulated at the information systems level. Based on the work on I.S. and software modelling we should come with such a taxonomy by making a distinction between assets associated with:

- the environment of the information systems: persons, buildings etc;
- software artefacts: components of various types (programs, database, HCI, etc) belonging to the application, middleware and operating system levels;

- physical artefacts: hardware, networks, etc.

In order to explore this taxonomy, we need to consider different sources in terms of meta-models associated with different proposed modelling languages tackling different perspectives (or viewpoints) of the IS:

- the business perspective associated with an IS: UML (use cases, activity diagrams, etc.), UEML (the IS modelling part of it), CIM (from MDA), etc.
- the software perspective: MDA (PSM, PIM), ADL (Architectural Description Languages) like ACME, xADL, ODP architecture and reference model [L95], etc.
- the physical perspective: UML deployment diagram, etc.

The objective is here to consolidate all the relevant aspects of these models in order to come with a complete ontology of all the resources that are part of an IS and to which security vulnerabilities can be associated. The work on this part requires close links and cooperation with the INTEROP DEM and DAP JR activities.

II.6.1.3 Security qualities

Central in the framework presented at the beginning of this section is the identification of the security qualities. There we need also to come up with a taxonomy of these security qualities so that their semantics can be clarified as well as stating the interrelation existing between some of them. Different sources for establishing such taxonomy exist, like:

- Software qualities: Security qualities can be derived from several different software quality models and standards including catalogues like ISO/IEC 9126 Standard for Quality Models, IEEE 1061 Standard for a Software Quality Metrics Methodology, different attribute catalogues, etc.
- Security properties: Those can be found in different security norms like the Common Criteria or IS0 17799. They can also be derived from some ‘standard’ templates used for requirements engineering. Such templates always include a so-called NFR (Non Functional Requirements) part and can be found in standardized documents like those proposed in ANSI-IEEE 830-1998, ESA PSS-05-0, etc.

Another issue is related to the scope of the so-called security properties. The more traditional view associates security quality with those of Confidentiality, Integrity Authentication and Non-reputation. At a larger extent, more recently, some authors consider Availability as a required property. It is clear that considering this last quality as a security property opens the door to the inclusion of a larger set of additional qualities like Reliability, Performance, etc. Work around these issues is clearly related to the work performed in the sub-task TG 7.2.3.

II.6.2 Identification of specific issues of interoperability

In the previous section, we have listed the ingredients underlying the set-up of a framework supporting the management of security risks through the alignment of business and IS assets. As detailed in the previous section, two of these ingredients are:

- A taxonomy of business assets together with the identification of their associated economic value.

- A taxonomy of information systems assets according to an enterprise, software and physical (deployment) perspective.

As the information system is the mirror of the business, it is essential to be able to trace all the business assets in terms of their IS assets counterparts. For example, information about customers of a business needs to be traced to specific databases where data about customers is stored, networks over which customers' data is transmitted or secretarial staff encoding data about these customers. All are IS assets (resources) that are linked to business assets. In order to identify them for the purpose of securing them we need to establish a global matrix between the business and IS assets.

The development of this matrix follows some principles underlying research in terms of Business/IT alignment. The seminal work in the field has been done by Henderson and Venkatraman [HV99]. The most important view on business/IT alignment is represented in the following diagram.

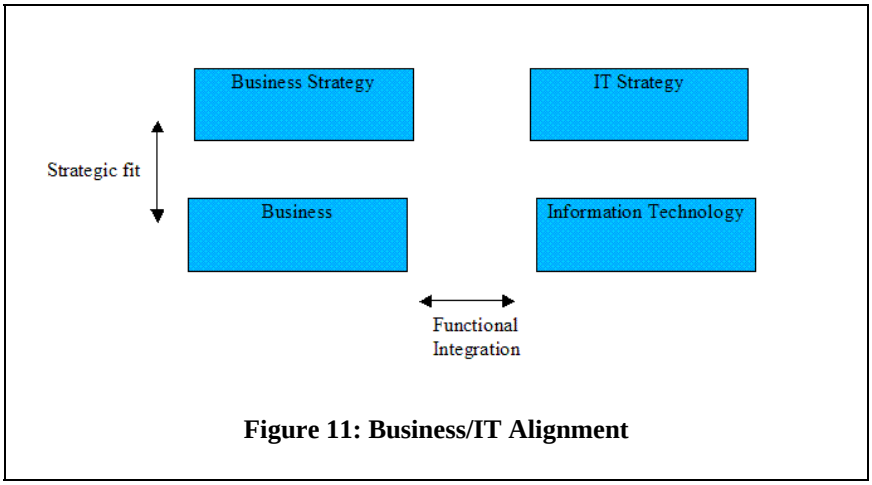

Figure 11: Business/IT Alignment

There is a functional dependency between the left side (business side) of this picture and the right side (Information Technology view). In this view, Information Technology corresponds to the information system support described above in this section.

Finding methods for improving the Business/IT alignment is still a hard problem. In order to understand more deeply the best practices, some work has been done in the field of business/IT alignment assessment [L00]. The research on assessment models could lead to the discovery of key success indicators of the business/IT alignment. In INTEROP, TG5 is working on these issues.

Within our context, the impact of this research and of on-going work will be limited to the understanding of

- the relation at the functional level, i.e. the alignment between the business (business process models) and the information technology (information system models).
- the relation between the economic value of economic artefacts and its link with the manipulation of these artefacts at the IS level.

This is shown in the following diagram.

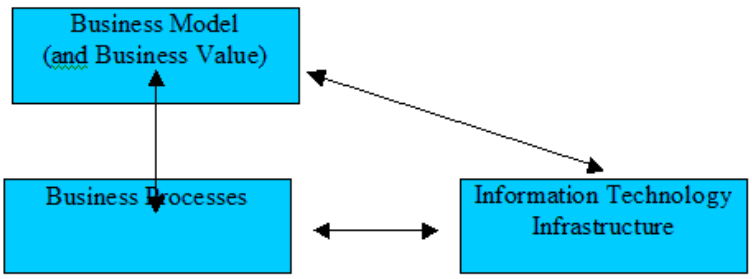

Figure 12: Future directions

Basically at this level we need to establish a new global meta-model (or ontology) connecting the different partial meta-models (associated with the three components). This meta-model should guarantee the global traceability that needs to be established between the different artefacts. Furthermore it should be able to accommodate evolution of the business value of business artefacts, the business processes operationalizing the business goals and the IS supporting the business are supposed constantly to be modified and updated over time.

II.6.2.1 Value modelling and enterprise architecture

ICT-based services are increasingly being developed and provided by networks of cooperating organizations. Various studies (see, e.g., [BE93]) indicate, however, that companies encounter serious difficulties in achieving the anticipated benefits from cooperation. Given the disappointing success rates of inter-firm co-operations and the risks and cost involved in the introduction of new ICT supported services, it is not surprising that practitioners and academics pay a great deal of attention to the concept of system interoperability. By system interoperability we understand the interoperability of actual, implemented systems and we use the term system in a broad sense: not only technical systems, but also organisational systems. We anticipate that business value modelling and enterprise architecture can blend into an integral approach for modelling e-services, thus playing an important role in the way system interoperability is addressed. One of the main issues today is that business value models do not stand by themselves, but relate to many other perspectives, such as inter-organizational business processes and supporting ICT. How to relate these perspectives is still a matter of debate since many researchers (see, e.g., [T01]; [GA01]) only focus on the actors, relationships, and value objects exchanged. However, enterprises can be viewed as complex “systems” with multiple domains (business value, process, ICT) that may influence each other. In general, architectures are used to describe components, relations and underlying design principles of a system [IEEE00]. Constructing architectures for enterprises may help to increase insight and the overview required to aligning the business and ICT successfully [L05], thus filling the gap between business value models and business strategy on the one hand, and business architecting on the other hand. Although the value of architecture has been recognised by many organisations, generally separate architectures are constructed for various organisational domains, such as business value, processes, applications, information and technical infrastructure. The relations between these architectures often remain unspecified or implicit. This is where model-driven (enterprise) architecture and business modelling methodologies can play a role. In general,

business models focus on the service value generated by a business, whereas enterprise architecture models show how a business realises these services, within or across the organizational borders. Linking these approaches, possibly using model transformation techniques, may result in a powerful modelling and analysis tool that integrates the inter-organizational value exchange models and the architectural models that are required to design these services. One approach that makes a first step in his direction [vBJG05], is building upon the *e*^{3}*-value* method [GA01] for business model analysis and the ArchiMate language [L05] allowing the linkage of revenues and cost in a single model.

II.6.3 Specific proposals for future work in the INTEROP framework

In the previous sections we have discussed the need for the development of a global ontology, connecting business assets (with their associated economic value) to IS assets. The creation of this ontology is a prerequisite for the added-value part of the security risk management that is related to the decision taking process. This process is associated with the decision about which protection (security counter-measures) should be established within the system for protecting IS assets themselves mirroring business assets having some business value. In short, the reasoning is the following: what are the vulnerabilities and the potential threats associated with each IS asset, and what are the impacts of the exploitation of these vulnerabilities on the business assets? As each business asset has an associated economic value, this impact can be fully qualified.

In order to support such a line of reasoning we propose to use requirements engineering (RE) and architectural engineering (AE) techniques for supporting a formal and systematic approach.

The overall approach is summarized in Figure 13, which complements the one presented in the first section. Besides the use of models based on adequate ontologies for representing the business and IS assets, we have introduced a central component that is related to “security requirements”. These security requirements are related to security qualities described in the previous section together with some possible associated taxonomy.

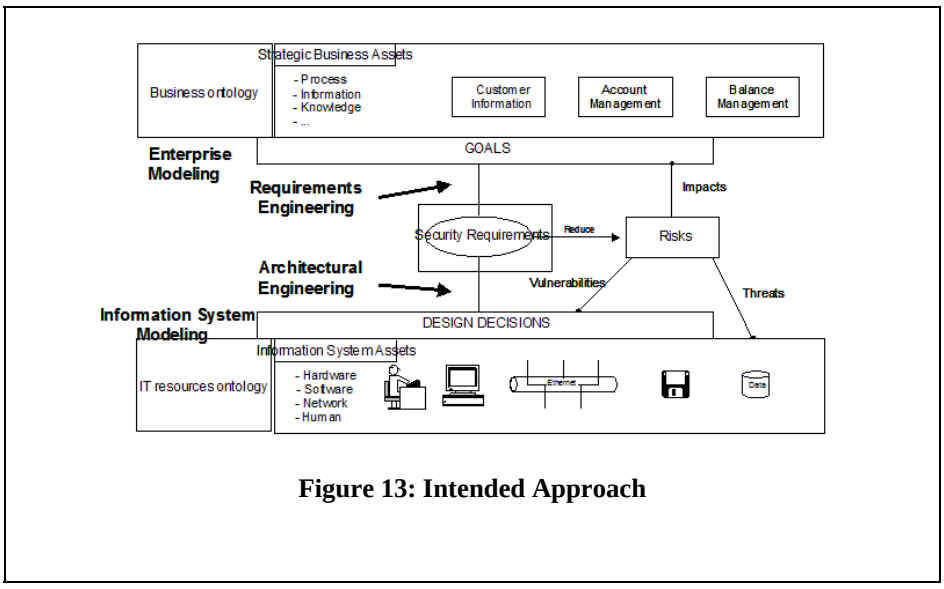

Figure 13: Intended Approach

- Requirements engineering techniques should be used for eliciting and formalizing the security requirements. In particular, the so-called "goal-oriented" techniques like those proposed in the Kaos-Grail [vLBDLJ03] [vL04] and i* [LYM03] [YC02] frameworks are proposed to understand the high-level security goals associated with the business and to derive finer security requirements from them in a systematic and structured way. In the proposed approach the high-level goals should be associated with the business assets and the hierarchy of goals should reflect the economic value of these business assets. At the lower level, goals are also associated with IS assets as they are the mirror of the business assets. More about this approach can be found in [MRD05].
- When security requirements have been established, formal reasoning should start in order to take appropriate design decisions regarding the security components to be introduced in the IS architecture. For a single security requirement, several alternatives can exist in terms of security components. For example an IDS component or a firewall component are two possible solutions for a same security requirement. However each solution has a specific cost in terms of development/acquisition, configuration and maintenance. Therefore the architectural design decision should be accompanied by a systematic risk-based analysis process. What are the pros and cons of each possible solution with respect their impact on the business? To this end, we need to come with a clear ROI regarding the overall cost of the solution and the economic value of the business asset that is protected. To support this approach we need to use architectural engineering techniques which support a systematic handling of non-functional requirements (like [C93] and [CNY94a], [CNY94b]) and complement them with risk mitigation approaches like those proposed in [MKKA03].

II.6.4 Dependencies and benefits from these actions

As the result of this presentation one can see that the proposed work relies more on the integration of different techniques and research results than on the development of a new branch of research. The added value results from the creation of an adequate framework for integrating these different results and its application to the domain of risk-based security IT management. We think that this action should play a role of catalyst by linking different techniques and results, most of them being produced within the INTEROP context, namely:

- Ontologies for representing business and enterprise assets (DEM: Domain Enterprise Modeling) and for representing IS and software systems assets (DAP: Domain Architecture and Platforms), the whole approach is being supported through DO (Domain Ontologies) techniques. Activities should also benefit from the consolidation of all these works through TG2 (Model-driven interoperability) results.
- Security qualities and non-functional requirements taxonomies based on the work performed in the sub-task TG 7.2.3.
- Work on value, business process and IS alignment performed in TG5.

II.7 Acronyms

ACID	Atomic, Consistent, Independent and Durable
ACME	CMU Architecture Description Environment
XADL	Highly Extensible Architecture Description Language (from UC Irvine)
AE	Architectural Engineering
ANSI	American National Standards Institution
AOP	Aspect Oriented Programming
ATHENA	Advanced Technologies for interoperability of Heterogeneous Enterprise Networks and their Applications
B2B	Business to Business
BCA	Business Contract Architecture
BCL	Business Contract Language
BID	Bid
BPML	Business Process Modelling Language
BSI	Bundesamt für Sicherheit in der Informationstechnik, British Standards Institution
BTP	Business Transaction Protocol
CACM	Communications of the Association for Computing Machinery
CAS	Contractual Agent Societies
CCO	Chief Compliance Officer
CD	Compact Disc
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CIM	Computation Independent Model
CIO	Chief Information Officer
CNP	Contract Net Protocol
COO	Chief Operating Officer
CORBA	Common Object Request Broker Architecture
COSMOS	Cluster Of Systems of Metadata for Official Statistics
CPA	Collaboration Profile Agreement
CRAMM	Common Risk Analysis and Management Method
CSO	Chief Security Officer
CTO	Chief Technical Officer
DAI	Distributed Artificial Intelligence
DAP	Dommain Architectures and Platforms
DEM	Domain Enterprise Modelling
DO	Domain Ontologies
DPM	Digital Policy Management
DRM	Digital Rights Management

DVD	Digital Versatile Disc
EAI	Enterprise Application Integration
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
ebXML	Electronic Business using eXtensible Markup Language
EDEE	E-commerce application Development and Execution Environment
EDI	Electronic Data Interchange
EPC	Event Process Chains
ERP	Enterprise Resource Planning
ESA	European Space Agency
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
HCI	Human Computer Interaction
HIPAA	Health Insurance Portability and Accountability Act of 1996
HR	Human Resources
IBM	International Business Machines
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IFPI	International Federation of Phonographic Industry
INTEROP	Interoperability Research for Networked Enterprises and Software
IS	International Standard
ISO	International Organization for Standardization
IT	Information Technology
JR	Joint Research; Japanese Railways
KMS	Knowledge Management System
MDA	Model Driven Architecture (TM OMG)
MDD	Model Driven Development
META	The META Group is now part of Gartner's.
MOM	Message Oriented Middleware
MPEG	Motion Picture Experts Group
MTCO	Multi Tier Contract Ontology
NASD	National Association of Securities Dealers
NFA	Non-Functional Aspects
NFR	Non-Functional Requirements
ODP	Open Distributed Processing
ODRL	Open Digital Rights Language
OMA	Object Management Architecture; Open Mobile Alliance

P2P	Peer to Peer
P3P	Platform for Privacy Preferences
PAMELA	Petri-net based Activity Management Execution Language
PDA	Personal Digital Assistant
PIM	Platform Independent Model
PSM	Platform Specific Model
PSS	Procedures, Specifications and Standards
R&D	Research and Development
RDD	Rights Data Dictionary
RE	Requirements Engineering
REL	Rights Expression Language
RFB	Request For Bids
ROI	Return on Investment
RuleML	Rule Markup Language
SAML	Security Assertion Markup Language
SB	Security Breach (as in California Security Breach Information Act (SB-1386))
SIMAP	Système d'Information pour les Marchés Publics
SOX,	Sarbanes-Oxley
T-SAS	see [LBLB05]
TFI	Technical, Formal and Informal
TG	Task Group
TPA	Trading Partner Agreement
TRACONET	Transportation Cooperation Net
UEML	Unified Enterprise Modelling Language
UML	Unified Modelling Language
UPS	United Parcel Service
USB	Universal Serial Bus
VPN	Virtual Private Network
WP	Work Package
WS	Web Services
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

II.8 Bibliography

[Å02] R.-M. Åhlfeldt. Information security in home healthcare; a case study. In M. Warren and J. Barlow, editors, *Proceedings of the Third International Conference of the Australian Institute of Computer Ethics (AiCE)*, pages 1–10, Sydney, Australia, September 2002.

[ÅA04] R-M. Åhlfeldt and L. Ask. Information security in electronic medical records: A case study with the user in focus. In *Proceedings of the Information Resources Management Association International Conference*, pages 345–347, New Orleans, USA, May 2004.

[AEB02] A. Abrahams, D. Eyers, and J. Bacon. An asynchronous rule-based approach for business process automation using obligations. In *Third ACM SIGPLAN workshop on Rule Based Programming (RULE02)*, 2002.

[AG01] S. Angelov and P. Grefen. B2B e-contract handling – a survey of projects, papers and standards. Technical Report 01-21, CTIT, University of Twente, 2001.

[AG03a] S. Angelov and P. Grefen. The 4W framework for B2B e-contracting. *Int. J. Networking and Virtual Organisation*, 1(3), 2003.

[AG03b] S. Angelov and P. Grefen. An analysis of the B2B e-contracting domain – paradigms and required technology. Technical Report WP102, Eindhoven University of Technology, 2003.

[ÅN05] R-M. Åhlfeldt and M. Nohlberg. System and network security in a heterogenous healthcare domain: A case study. In *Proceedings of the 2005 Security Conference*, Las Vegas, USA, March 2005.

[ARH98] A. Abdul-Rahman and S. Hailes. A distributed trust model. In *Proceedings of the New Security Paradigms workshop*, pages 48–60, Langdale, Cumbria, UK, 1998. ACM Press. Available from: `http://doi.acm.org/10.1145/283699.283739`.

[ARH00] A. Abdul-Rahman and S. Hailes. Supporing trust in virtual communities. In *Hawai International Conference on System Sciences*, Maui, Hawaii, 2000.

[AW05] S. Artyshchev and H. Weigand. Contract-based interoperability for e-business transactions. In *Proc. INTEROP-ESA*, Geneva, 2005.

[BBGR03] E. Becker, W. Buhse, D. Günnewig, and N. Rump, editors. *Digital Rights Management, Technological, Economic, Legal and Political Aspects*, volume 2770 of *Lecture Notes in Computer Science*. Springer-Verlag, 2003.

[BE93] L. Bleeke and D. Ernst. The way to win in cross border alliances. In J. Bleeke and D. Ernst, editors, *Collaborating to Compete: Using Strategic Alliances an Acquisitions in the Global Marketplace*. Wiley, New York, 1993.

[BFK98] M. Blaze, J. Feigenbaum, and A.D. Keromytis. KeyNote: Trust management for public-key infrastructures. In *Proceedings of 6th International Workshop on Security Protocols*, volume 1550 of *Lecture Notes in Computer Science*, pages 59–63, Cambridge, UK, April 1998. Springer-Verlag. Available from: `http://www.springerlink.com/link.asp?id=6ku13fr5jt3mgdxk`.

[BFL96] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized trust management. In *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE, 1996. Available from: `http://ieeexplore.ieee.org/iel3/3742/10940/00502679.pdf`.

[BLB03] Sonja Buchegger and Jean-Yves Le Boudec. The effect of rumor spreading in reputation systems for mobile, ad hoc and wireless neworks. In *Proc. WiOpt'03 (Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks)*, Sophia-Antipolis, France, 2003.

[C92] R.V. Clarke, editor. *Situational Crime Prevention: Successful Case Studies*. Harrow and Heston, Albany, NY, 1992.

[C93] Lawrence Chung. Dealing with security requirements during the development of information systems. In *Proceedings of Advanced Information Systems Engineering*, pages 234–251, June 1993.

[C94] Brad Cox. Superdistribution. *Wired Magazine*, pages 89–92, September 1994.

[C96] Brad Cox. *Superdistribution, Objects as property on the Electronic Frontier*. Addison-Wesley, 1996.

[C02] C. Ciborra. *The Labyrinths of Information: Challenging the Wisdom of Systems*. Oxford University Press, Oxford, 2002.

[C+03] V. Cahill et al. Using trust for secure collaboration in uncertain environments. *Pervasive Computing*, 2(3):52–61, 2003.

[CFL+97] Y.-H. Chu, J. Feigenbaum, B. LaMacchia, P. Resnick, and M. Strauss. REFEREE: Trust management for web applications. *Computer Networks and ISDN Systems*, 29(8–13):953–964, 1997.

[CNY94a] L. Chung, B.A. Nixon, and E. Yu. Using quality requirements to drive software development. In *Workshop on Research Issues in the Intersection Between Software Engineering and Artificial Intelligence*, Sorrento, Italy, May 1994.

[CNY94b] L. Chung, B.A. Nixon, and E. Yu. Using quality requirements to systematically develop quality software. In *Proceedings of the Fourth International Conference on Software Quality*, McLean, VA, USA, October 1994.

[Cor04] *The CORAL Consortium*, 2004. Available from: `http://www.coral-interop.org/`.

[CS01] M. Chen and J.P. Singh. Computing and using reputations for internet ratings. In *Proceedings of the 3rd ACM conference on Electronic Commerce*, pages 154–162. ACM Press, 2001.

[CW85] Luca Cardelli and Peter Wegner. On understanding types, data abstraction, and polymorphism. *Computing Surveys*, 17(4):471–522, December 1985.

[D97a] A. Daskalopulu. Logic based tools for legal contract drafting: Prospects and problems. In *Proceedings of the 1st Logic Symposium*, pages 213–222. University of Cyprus Press, 1997.

[D97b] G. Dhillon. *Managing information system security*. Macmillan, London, 1997.

[D02] A. Daskalopulu. Evidence based electronic contract performance monitoring. *The INFORMS Journal of Group Decision and Negotiation. Special Issue on Formal Modelling in E-Commerce*, 2002.

[DA04] Zoran Despotovic and Karl Aberer. Maximum likelihood estimation of peers' performance in P2P networks. In *Second Workshop on the Economics of Peer-to-Peer Systems*, 2004.

[DBG00] A. Durante, D. Bell, and L. Goldstein. A model for the e-service marketplace. Technical report, HP Laboratories, Palo Alto, 2000.

[DCH04] T.S. Dillon, E. Chang, and F.K. Hussain. Managing the dynamic nature of trust. *IEEE Journal Of Intelligent Systems*, pages 79–82, Sept/Oct 2004.

[DD05] Prashant Dewan and Partha Dasgupta. Securing P2P networks using peer reputations: Is there a silver bullet? In *IEEE Consumer Communications and Networking Conference (CCNC 2005)*, Las Vegas, 2005.

[DDLS01] N. Damianou, N. Dulay, E. Lupu, and M. Sloman. The Ponder policy specification language. In *Workshop on Policies for Distributed Systems and Networks (Policy2001)*, volume 1995 of *Lecture Notes in Computer Science*, HP Labs Bristol, January 2001. Springer-Verlag. Available from: `http://www.springerlink.com/link.asp?id=1r0vn5hfxk6dxebb`.

[DK99a] C. Dellarocas and M. Klein. Civil agent societies: Tools for inventing open agent-mediated electronic marketplaces. In *Proceedings of the Workshop in Agent-Mediated Electronic Commerce (co-located with IJCAI'99)*, Stockholm, Sweden, July 1999.

[DK99b] C. Dellarocas and M. Klein. Designing robust, open electronic marketplaces of contract net agents. In *Proceedings of the 20th International Conference on Information Systems (ICIS)*, Charlotte, NC, December 1999.

[DK00] C. Dellarocas and M. Klein. An experimental evaluation of domain-independent fault handling services in open multi-agent systems. In *ICMAS-2000, The International Conference on Multi-Agent Systems*, 2000.

[DM01] A. Daskalopulu and T.S.E. Maibaum. Towards electronic contract performance. Legal information systems applications. In *12th International Conference and Workshop on Database and Expert Systems Applications*, page 771. IEEE C. S. Press, 2001.

[DR03] C. Dellarocas and P. Resnick. Online reputation mechanisms: A roadmap for future research. Technical report, MIT, 2003.

[DS97] A. Daskalopulu and M.J. Sergot. The representation of legal contracts. *AI and Society*, 11(1–2):6–17, 1997.

[DWR04] T. Dimitrakos, M. Wilson, and S. Ristol. TrustCoM – a trust and contract management framework enabling secure collaborations in dynamic virtual organisations. *ERCIM News*, 59, October 2004. Available from: `http://www.ercim.org/publication/Ercim_News/enw59/dimitrakos2.html`.

[F03] Edward W. Felten. A skeptical view of DRM and Fair Use. *Communications of the ACM*, 46(4):57–59, 2003.

[FL89] D. Fudenberg and D. Levine. Reputation and equilibrium selection in games with a patient player. *Econometrica*, 57(4):759–778, 1989.

[FS03] B.S. Firozabadi and M.J. Sergot. Revocation in the privilege calculus. In *Workshop on Formal Aspects of Security and Trust (FAST2003)*, pages 39–51, Italy, 2003. IIT-CNR. TR-10/2003.

[G99] M. Griss. My agent will call your agent – but will it respond? Technical report, HP Laboratories, Palo Alto, 1999.

[G00] D. Gambetta. Can we trust trust? In *Trust: Making and Breaking Cooperative Relations*, pages 213–237. Department of Sociology, University of Oxford, 2000. Available as http://www.sociology.ox.ac.uk/papers/gambetta213-237.pdf.

[GA01] J. Gordijn and H. Akkermans. Designing and evaluating e-business models. *IEEE Intelligent Systems*, 16(4):11–17, 2001.

[GBW+98] F. Griffel, M. Boger, H. Weinreich, W. Lamersdorf, and M Merz. Electronic contracting with COSMOS - how to establish, negotiate and execute electronic contracts on the Internet. In *Proceedings of Second International Enterprise Distributed Object Computing Workshop (EDOC '98)*, 1998.

[GHM00] A. Goodchild, C. Herring, and Z. Milosevic. Business contracts for B2B. In *Proceedings of the CAISE00 Workshop on Infrastructure for Dynamic Business-to-Business Service Outsourcing*, 2000.

[GKRT04] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins. Propagation of trust and distrust. In *Proceedings of the Thirteenth International World Wide Web Conference*, pages 403–412, New York, May 2004. ACM. Available from: `http://www.www2004.org/proceedings/docs/1p403.pdf`.

[GLC99] B.N. Grosof, Yannis Labrou, and Hoi Y. Chan. A declarative approach to business rules in contracts: Couteous logic programs in XML. In *Proceedings of 1st ACM Conference on Electronic Commerce (EC99)*, 1999.

[GMMZ05] P. Giorgini, F. Massacci, J. Mylopoulos, and N. Zannone. Modeling social and individual trust in requirements engineering methodologies. In *Third International Conference on Trust Management, iTrust 2005*, volume 3477 of *Lecture Notes in Computer Science*, pages 161–176,

Paris, France, May 2005. Springer-Verlag. Available from: http://www.springerlink.com/link.asp?id=wbtuqt1n8bbhde40.

[GN05] Martin Gudgin and Anthony Nadalin. *Web Services Trust Language (WS-Trust)*, February 2005. Available from: ftp://www6.software.ibm.com/software/developer/library/ws-trust.pdf.

[GP03] B N. Grosof and T. Poon. SweetDeal: Representing agent contracts with exceptions using XML rules, ontologies and process descriptions. In *Proc. Intl. Conf. on the World Wide Web*, 2003.

[GS00] T. Grandison and M. Sloman. A survey of trust in Internet applications. *IEEE Communications Surveys and Tutorials*, 3(4):2–16, 2000. Available from: http://www.comsoc.org/livepubs/surveys/public/2000/dec/grandison.html.

[GS01] T.W.A. Grandison and M. Sloman. Sultan - a language for trust specification and analysis. In *Eight Workshop of the HP OpenView University Association*, Berlin, June 2001. Available from: http://www.hpovua.org/PUBLICATIONS/PROCEEDINGS/8_HPOVUAWS/Papers/Paper01.2-Grandison-Sultan.pdf.

[HDA03] M. Hauswirth, A. Datta, and K. Aberer. Handling identity in peer-to-peer systems. In *6th International Workshop on Mobility in Databases and Distributed Systems, in conjunction with the 14th International Conference on Database and Expert Systems Applications*, September 2003.

[HV99] Henderson and Venkatraman. Strategic alignment : Leveraging information technology for transforming organizations. *IBM Systems Journal*, 38:472–484, 1999.

[I02] R. Iannella. *Open Digital Rights Language (ODRL), Version 1.1*. World Wide Web Consortium, September 2002. Available from: http://www.w3.org/TR/odrl/.

[IEEE00] IEEE Computer Society, New York. *IEEE Std 1471-2000: IEEE Recommended Practice for Architectural Description of Software-Intensive Systems*, 2000.

[IJ05] M.-E. Iacob and H. Jonkers. Quantitative analysis of enterprise architectures. In *First International Conference on Interoperability of Enterprise Software and Applications (INTEROP-ESA'05)*, Geneva, Switzerland, February 2005.

[ISO04a] *ISO 21000-5: Information Technology – Multimedia Framework (MPEG-21) – Part 5: Rights Expression Language*, 2004.

[ISO04b] *ISO 21000-6: Information Technology – Multimedia Framework (MPEG-21) – Part 6: Rights Data Dictionary*, 2004.

[itr05] *iTrust Working Group on Trust Management in Dynamic Open Systems*, 2005. Available from: http://www.itrust.uoc.gr/.

[J96] A. Jøsang. The right type of trust for computer networks. In *Proceedings of the ACM New Security Paradigms Workshop*. ACM, 1996. Available from: http://security.dstc.edu.au/staff/ajosang/papers/trdsyst.ps.

[JILS05] H. Jonkers, M.-E. Iacob, M. Lankhorst, and P. Strating. Integration and analysis of functional and non-functional aspects in model-driven e-service development. In *Proceedings 9th IEEE International EDOC Enterprise Computing Conference*, pages 229–238, Enschede, the Netherlands, September 2005.

[JP05] A. Jøsang and S. Pope. Semantic constraints for trust transitivity. In *Proceedings of the Second Asia-Pacific Conference on Conceptual Modelling (APCCM 2005)*, volume 43 of *Conferences in Research and Practice in Information Technology*, pages 59–68, Newcastle, Australia, January 2005. ACS. Available from: http://crpit.com/confpapers/CRPITV43Josang.pdf.

[JSW98] N.R. Jennings, K. Sycara, and M. Wooldridge. A roadmap of agent research and development. *Autonomous agents and multi-agent system*, 1(1), 1998.

[KD99] M. Klein and C. Dellarocas. Exception handling in agent systems. In *Proceedings of the Third International Conference on Autonomous Agents*, Seattle, Washington, 1999.

[KD00] M. Klein and C. Dellarocas. Domain-independent exception handling services that increase robustness in open multi-agent systems. Technical Report ASES-WP-2000-02.m, Massachusetts Institute of Technology, Cambridge MA USA, 2000.

[KDJ05] V. Kabilan, J. Dzdrakovic, and P. Johannesson. Use of multi-tier contract ontology to deduce contract workflow models for enterprise interoperability. In *Proceedings of 2nd INTEROP-EMOI open workshop on Enterprise Models and Interoperability, collocated with CAISE 2005*, Porto, 2005.

[KDR01] K. Karlapalem, A R. Dani, and Krishna Radha. A framework for modelling electronic contracts. In *Proceedings of Entity Relationship and Conceptual Modelling (ER 2001)*, number 2224 in Lecture Notes in Computer Science, pages 193–207, Paris, France, 2001. Springer-Verlag.

[KJ03] V. Kabilan and P. Johannesson. Semantic representation of contract knowledge using multi-tier contract ontology. In *Proceedings of Semantic Web and Databases workshop (SWDB 2003)*, 2003.

[KJR03a] V. Kabilan, P. Johannesson, and D. Rugaimukammu. Business contract obligation monitoring through use of multi-tier contract ontology. In *Proceedings of Workshop on Regulatory Ontologies (Worm CoRe 2003)*, number 2889 in Lecture Notes in Computer Science, Italy, November 2003. Springer-Verlag.

[KJR03b] V. Kabilan, P. Johannesson, and D. Rugaimukammu. An ontological approach to unified contract management. In *Proceedings of 13th European Japanese Conference on Information Modelling and Knowledge Bases*, Kitakyushu, Japan, June 2003. IOS Press.

[KM97] S O. Kimbrough and S A. Moore. On automated message processing in e-commerce and work support systems: Speech act theory and expressive felicity. *Transactions on Information Systems*, October 1997.

[KM05a] H. Koshutanski and F. Massacci. Interactive credential negotiation for stateful business processes. In *Proceedings of Third International Conference on Trust Management (iTrust 2005)*, number 3477 in Lecture Notes in Computer Science, pages 256–272, Paris, France, May 2005. Springer-Verlag. Available from: `http://www.springerlink.com/link.asp?id=gkmnbpdccu0ammb1`.

[KM05b] Lea Kutvonen and Janne Metso. Services, contracts, policies and ecommunities – relationship to ODP framework. In *(WODPEC 2005) associated with the 9th IEEE International EDOC Enterprise Computing Conference*, Enschede, the Netherlands, September 2005.

[KMR05] Lea Kutvonen, Janne Metso, and Toni Ruokolainen. Inter-enterprise collaboration management in dynamic business networks. In *International Conference on Cooperative Information Systems (CoopIS 2005)*, Agia Napa, Cyprus, November 2005.

[KN03] Chris Kaler and Anthony Nadalin. *Web Services Federation Language (WS-Federation), Version 1.0*, July 2003. Available from: `http://www-106.ibm.com/developerworks/library/ws-fed/`.

[KRMH05] Lea Kutvonen, Toni Ruokolainen, Janne Metso, and Juha Haataja. Interoperability middleware for federated enterprise applications in web-Pilarcos. In *First International Conference on Interoperability of Enterprise Software and Applications (INTEROP-ESA'05)*, Geneva, Switzerland, February 2005.

[KSGM03] S. Kamvar, M. Schlosser, and H. Garcia-Molina. The EigenTrust algorithm for reputation management in P2P networks. In *Proceedings of the 12th International World-Wide Web Conference (WWW03)*, pages 446–458, May 2003. Available from: `http://www2003.org/cdrom/papers/refereed/p446/p446-kamvar/index.html`.

[KW82] D. Kreps and R. Wilson. Reputation and imperfect information. *Journal of Economic Theory*, 27:253–279, 1982.

[L88] R.M. Lee. A logic model for electronic contracting. *Decision Support Systems*, 4:27–44, 1988.

[L92] R.M. Lee. Facilitating international contracting: AI extensions to EDI. *International Information Systems*, January 1992.

[L95] P.F. Linington. RM-ODP: The architecture. In *Open Distributed Processing, Experiences with distributed environments. Proceedings of the 3rd IFIP TC 6/WG 6.1 International Conference on Open Distributed Processing (ICODP95)*, pages 15–33, Brisbane Australia, March 1995.

[L98] R.M. Lee. Towards open electronic contracting. *EM - Electronic Contracting. EM - Electronic Markets*, 8(3):10, 1998.

[L00] J.N. Luftman. Assessing business/IT alignment maturity. *Communications of AIS*, 4(14), 2000.

[L05] M. Lankhorst. *Enterprise Architecture at Work – Modelling, Communication and Analysis*. Springer-Verlag, 2005.

[LB90] Liebenau and Backhouse. *Understanding Information: An Introduction*. Macmillan, 1990.

[LMC+04] P. F. Linington, Z. Milosevic, J. Cole, S. Gibson, S. Kulkarni, and S. Neal. A unified behavioural model and a contract language for extended enterprise. *Data Knowledge and Engineering Journal*, 51(1):5–29, October 2004. Available from: `http://www.cs.kent.ac.uk/pubs/2004/1960`.

[LNO+04] Travis Leithead, Wolfgang Nejdl, Daniel Olmedilla, Kent E. Seamons, Marianne Winslett, Ting Yu, and Charles C. Zhang. How to exploit ontologies for trust negotiation. In *Workshop on Trust, Security, and Reputation on the Semantic Web*, Hiroshima, Japan, November 2004.

[LP01] P. Levine and J. Pomerol. From business modelling based on the semantics of contracts to knowledge modelling and management. In *Proceedings of 34th Annual Hawaii International Conference on System Sciences*, 2001.

[LPBLB05] S. Lo Presti, M. Butler, M. Leuschel, and C. Booth. A trust analysis methodology for pervasive computing systems. In *Trusting Agents for Trusting Electronic Societies*, number 3577 in Lecture Notes in Artificial Intelligence, pages 129–143. Springer-Verlag, 2005. Available from: `http://www.springerlink.com/link.asp?id=722hx4gcq3nx1vdq`.

[LYM03] L. Liu, E. Yu, and J. Mylopoulos. Security and privacy requirements analysis within a social setting. In *Proc. 11th IEEE International Requirements Engineering Conference*, 2003.

[M94] S. Marsh. *Formalising Trust as a Computational Concept*. PhD thesis, University of Stirling, Department of Computer Science and Mathematics, 1994.

[M04] Brian Matthews. *Framework for Security and Trust Standards: Experiments and Implementations*. SWAD-EUROPE (W3C Semantic Web Advanced Development for Europe, IST-2001-34732), July 2004. Available from: `http://www.w3.org/2001/sw/Europe/reports/trust/11.2/d11.2-implementation.html`.

[MC96] D.H. McKnight and N.L. Chervany. The meanings of trust. Technical report, University of Minnesota, MIS Research Center, 1996. Available from: `http://misrc.umn.edu/workingpapers/fullPapers/1996/9604_040100.pdf`.

[MD02] Z. Milosevic and R.G. Dromey. On expressing and monitoring behaviour in contracts. In *6th International Enterprise Distributed Object Computing Conference (EDOC)*, 2002.

[MG00] W.E. McCarthy and G. Geerts. The ontological foundation of REA enterprise ontology. Technical report, Michigan State University, USA, 2000. Available from: `http://www.msu.edu/user/mccarth4/rea-ontology/`.

[MJPD02] Z. Milosevic, A. Jøsang, M.A. Patton, and T. Dimitrakos. Discretionary enforcement of electronic contracts. In *Enterprise Distributed Object Computing Conference (EDOC)*, 2002.

[MK90] R. Mori and M. Kawahara. Superdistribution: The concept and the architecture. *Transaction of the IEICE*, E 73(7):1133–1146, July 1990.

[MKKA03] Mike Moore, Rick Kazman, Mark Klein, and Jai Asundi. Quantifying the value of architecture design decisions: Lessons from the field. In *Proc. 25th International Conference on Software Engineering (ICSE'03)*, 2003.

[MRD05] Nicolas Mayer, Andre Rifaut, and Eric Dubois. Towards a risk-based security requirements engineering framework. In *Proc. Workshop Requirements Engineering Foundations for Quality (REFSQ'05)*, Porto, 2005.

[MT87] R. Mori and S. Tashiro. The concept of software service system (SSS). *Transaction of the IEICE*, J70-D(1):70–81, January 1987.

[N86] Oscar Nierstrasz. What is the 'Object' in object-oriented programming? In *Proceedings of the CERN School of Computing*, volume CERN 87-04, pages 43–53, Renesse, the Netherlands, September 1986.

[N05] M. Nohlberg. Social engineering audits using anonymous surveys – conning the users in order to know if they can be conned. In *Proceedings of the 2005 Security Conference*, Las Vegas, USA, March 2005.

[OGP05] Alexander Osterwalder, Jaap Gordijn, and Yves Pigneur. *Comparing two Business Model Ontologies for Designing e-Busines Models and Value Constellations*. Bled, Slovenia, June 2005.

[OMA04] *Open Mobile Alliance DRM Specification, Version 2.0, Candidate Enabler*, July 2004. Available from: `http://www.openmobilealliance.org/release_program/drm_v20.html`.

[OP04] Alexander Osterwalder and Yves Pigneur. An ontology for e-business models. In Wendy Currie, editor, *Value Creation from E-Business Models*. Butterworth-Heinenmann, April 2004.

[P02] Benjamin C. Pierce. *Types and Programming Languages*. The MIT Press, Massachusetts Institute of Technology, Cambridge, Massachusetts 02142, February 2002.

[R03] E. Rissanen. Server based application level authorisation for Rotor. *IEE Proceedings on Software*, 150(5):291–295, 2003. Available from: `http://ieeexplore.ieee.org/iel5/5658/27969/01249339.pdf`.

[RK05] S. Ruohomaa and L. Kutvonen. Trust management survey. In *Proceedings of the iTrust 3rd International Conference on Trust Management*, Rocquencourt, France, May 2005. Springer-Verlag. Available from: `http://dx.doi.org/10.1007/11429760_6`.

[RKKC04] P. Radha Krishna, K. Karlapalem, and D.K.W. Chiu. An EREC framework for e-contract modelling, enactment and monitoring. *Data and Knowledge Engineering*, 51(1):31–58, 2004.

[RTM01] B. Rosenblatt, B. Trippe, and S. Mooney. *Digital Rights Management: Business and Technology*. Hungry Minds/John Wiley and Sons, New York, 2001.

[S80] R.G. Smith. The Contract Net Protocol: High-level communication and control in a distributed problem solver. *IEEE Trans. On Computers*, C-29(12):1104–1113, 1980.

[S93] T. Sandholm. An implementation of the Contract Net Protocol based on marginal cost calculations. In *Eleventh National Conference on Artificial Intelligence (AAAI-93)*, pages 256–262, Washington DC, 1993.

[S96] M. Stefik. Letting loose the light: Igniting commerce in electronic publication. In M. Stefik, editor, *Internet Dreams: Archetypes, Myths and Metaphors*. MIT Press, Cambridge, MA, 1996.

[S04] Morris Sloman. Trust management in Internet and pervasive systems. *IEEE Intelligent Systems*, 19(5):77–79, September 2004.

[SD81] R.G. Smith and R. Davis. Frameworks for co-operation in distributed problem solving. *IEEE Trans. on System. Man and Cybernetics*, 11(1):61–70, 1981.

[SDN+00] M. Sachs, A. Dan, T. Nguyen, et al. Executable trading-partner agreements in electronic commerce. Technical report, IBM Research, 2000.

[SE03] J. Skene and W. Emmerich. A model driven architecture approach to non-functional analysis of software architectures. In *Proceedings 18th IEEE Conference on Automated Software Engineering (ASE'03)*, Toronto, Canada, October 2003.

[SJL03] M. Schoop, A. Jertila, and T. List. Negoisst: A negotiation support system for electronic business-to-business negotiations in e-commerce. *Data and Knowledge Engineering*, 47(3):371–401, 2003.

[SL95] T. Sandholm and V. Lesser. Issues in automated negotiation and electronic commerce: Extending the contract net framework. In *First International Conference on Multiagent Systems (ICMAS-95)*, pages 328–335, San Francisco, 1995.

[SL96] T. Sandholm and V. Lesser. Advantages of a levelled commitment contracting protocol. In *Thirteenth National Conference on Artificial Intelligence (AAAI-96)*, pages 126–133, Portland, OR, 1996.

[SMB05] Monica Scannapieco, Paolo Missier, and Carlo Batini. Data quality at a glance. *Datenbank-Spektrum*, 14:6–14, 2005.

[SS01] J. Sabater and C. Sierra. REGRET: A reputation model for gregarious societies. In *4th Workshop on Deception Fraud and Trust in Agent Societies*, Montreal, Canada, 2001.

[SSR+05] D. Simmonds, A. Solberg, R. Reddy, R. France, and S. Ghosh. An aspect oriented model driven framework. In *Proceedings of the 9th EDOC Enterprise Computing Conference*, pages 119–130, Enschede, the Netherlands, September 2005.

[ST04] Girish Suryanarayana and Richard N. Taylor. A survey of trust management and resource discovery technologies in peer-to-peer applications. Technical report, ISR, 2004.

[T01] D. Tapscott. Rethinking strategy in a networked world (or why Michael Porter is wrong about the Internet). *Strategy + Business*, 24(Third Quarter):1–8, 2001.

[TBJ+03] Gianluca Tonti, Jeffrey M. Bradshaw, Renia Jeffers, Rebecca Montanari, Ninrajan Suri, and Andrzej Uszok. Semantic web languages for policy representation and reasoning: A comparison of KAoS, Rei and Ponder. In *The SemanticWeb - ISWC 2003*, number 2870 in Lecture Notes in Computer Science, pages 419–437. Springer-Verlag, 2003. Available from: `http://www.springerlink.com/link.asp?id=bjhy2d977gf4e3qw`.

[TD04] Santtu Toivonen and Grit Denker. The impact of context on the trustworthiness of communication: An ontological approach. In *ISWC Workshop on Trust, Security, and Reputation on the Semantic Web*, 2004.

[TSA03] *Trust issues in pervasive environment*, September 2003. (Deliverable WP2-01), Trusted Software Agents and Services for Pervasive Information Environment project. Available from: `http://www.trustedagents.co.uk/TSA-WP2-01v1.1.pdf`.

[TT98] Yao-Hua Tan and Walter Thoen. Modeling directed obligations and permission in trade contracts. In *31st Annual Hawaii International Conference on System Sciences*, volume 5, 1998.

[TT02] Yao-Hua Tan and W. Thoen. Using event semantics for modeling contracts. In *Proceedings of 35th Hawaii International Conference on System Sciences*, 2002.

[TT03] Yao-Hua Tan and W. Thoen. Electronic contract drafting based on risk and trust assessment. *IJEC*, 7(4):55–72, 2003.

[V97] Egon Verharen. *A language-action perspective on cooperative information agents*. PhD thesis, Tilburg University, 1997.

[V05] L. Viljanen. Towards an ontology of trust. In *Proceedings of the 2nd International Conference on Trust, Privacy and Security in Digital Business (TrustBus'05)*. Springer-Verlag, 2005. Available from: `http://dx.doi.org/10.1007/11537878_18`.

[vBJG05] R. van Buuren, W. Janssen, and J. Gordijn. Business case modelling for e-services. In *Proceedings of the 18th Bled eConference: eIntegration in Action*, Bled, Slovenia, June 2005.

[vL04] A. van Lamsweerde. Elaborating security requirements by construction of intentional anti-models. In *Proceedings 26th International Conference on Software Engineering (ICSE 2004)*, 2004.

[vLBDLJ03] Axel van Lamsweerde, Simon Brohez, Renaud De Landtsheer, and David Janssens. From system goals to intruder anti-goals: Attack generation and resolution for security requirements engineering. In *Proceedings of the RE'03 Workshop on Requirements for High Assurance Systems (RHAS'03)*, Monterey (CA), September 2003.

[VRK04] Lea Viljanen, Sini Ruohomaa, and Lea Kutvonen. The TuBE approach to trust management. In *Proceedings of the 3rd iTrust internal workshop*, 2004. Available from: `http://www.cs.helsinki.fi/group/tube/papers/vrk04itrustworkshop.pdf`.

[W03] M. Winslett. An introduction to trust negotiation. In *Trust Management: First International Conference, (iTrust 2003)*, number 2692 in Lecture Notes in Computer Science, pages 275–283, Heraklion, Crete, Greece, May 2003. Springer-Verlag. Available from: `http://www.springerlink.com/link.asp?id=ufuj17106khufcj2`.

[WSJ00] W.H. Winsborough, K.E. Seamons, and V.E. Jones. Automated trust negotiation. In *Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX '00)*, pages 88–102. IEEE, 2000. Available from: `http://ieeexplore.ieee.org/iel5/6658/17862/00824965.pdf`.

[XJ03] Lai Xu and Manfred A. Jeusfeld. Pro-active monitoring of electronic contracts. In *Proc. CAiSE '03*, number 2681 in Lecture Notes in Computer Science. Springer-Verlag, 2003.

[YC02] E. Yu and L. Cysneiros. Designing for privacy and other competing requirements. In *2nd Symposium on Requirements Engineering for Information Security (SREIS'02)*, Raleigh, North Carolina, October 2002.

[ZYI04] Qing Zhang, Ting Yu, and Keith Irwin. A classification scheme for trust functions in reputation-based trust management. In *International Workshop on Trust, Security, and Reputation on the Semantic Web*, Hiroshima, November 2004. Available from: `http://sunsite.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-127/paper6.pdf`.