5.1 ADVANCED COLLABORATIVE BUSINESS ICT INFRASTRUCTURES

Ricardo J. Rabelo
Federal University of Santa Catarina, BRAZIL, rabelo@das.ufsc.br
GSIGMA – Intelligent Manufacturing Systems Group, Department of Automation and Systems

This paper points out the need of advanced collaborative business ICT infrastructures (CBI) for CNOs, the requirements for the development of CBIs, and the technologies and trends considering CNO issues. The CBI devised in the ECOLEAD Project is also presented, showing how most of these requirements and emergent ICTs have been incorporated in it. This CBI – called *ICT-I* – is a distributed, open and security-embedded infrastructure, and it relies on the service oriented architecture paradigm. Its services are to be used under the on demand and pay-per-use models. The assessment of ICT-I, some conclusions and challenges are presented in the end.

1. INTRODUCTION

The adoption of the Collaborative Networks Organizations (CNO) paradigm by organizations has been imposing an increasing and tremendous pressure on the companies´ competitive matrix, directly affecting their market positioning in terms of general quality, diversity and innovation of processes and products, prices, delivery dates, and level of relationship with suppliers and customers.

Nevertheless, in order to support the CNO concept realization, three essential pre-conditions are necessary to exist. The first one is that it requires *collaboration* among involved partners at a level far beyond sending e-mail messages. The second one is the existence of *trust*, considering that partners shall rely on each other (at variable levels). The third pre-condition is that all (or most of) the activities carried out within a CNO should be made via computer networks, i.e. *digital transactions* should be the routine, and not an exception.

Although the expression "working collaboratively" has been largely used by people and several authors, practice shows, however, that embedding this into the companies' daily business life impose drastic changes at all of their levels. Part of the changes is related to the difficulties related the *collaborative business infrastructures* (CBI) that are requested to support those pre-conditions.

In essence, a CBI for CNOs should be transparent, enabling networked organizations to agilely define and set up relations with other organizations seamlessly, and to be adaptive according to the business environment conditions and current organizations' autonomy levels (Camarinha-Matos and Afsarmanesh, 2004). This means having a CBI where businesses and collaboration can be accomplished more effectively, agilely, flexibly and trustworthily. Developing such kind of infrastructure is a key step towards creating an organization culture where collaboration can become part of the process and not only an option of work. More than this, it can help in making managers indeed confident and enthusiastic to use it in the support of their daily networked businesses as long as they realize the value added of such support.

Another fundamental facet about this issue is related to the different natures and sizes of the companies that typically are members of CNOs. In Europe, for example, more than 98% of them are SMEs[1]. As such, most of them have enormous difficulties to have access to the main products of the market as they require high investment in supporting software, hardware and IT experts.

Despite the complexity the development of such kind of CBI represents, the fact is that current solutions neither attend these requirements at all nor offer adequate support to CNO-related business processes. Moreover, they use to be complex to deploy and to use, they require powerful computing environments, they are usually expensive and not open, they require additional packages of security, and they are offered as huge packages of software no matter how much of this will be used. In other words, they preponderantly look to large companies and not to SMEs too.

This is the essential motivation of this paper, which presents the *concepts* of the CBI devised in the ECOLEAD project to cope with these requirements, and which can be affordable to SMEs. This paper is organized as follows. Chapter 1 highlights the need of CBIs for CNO, and presents requirements for that as well as some obstacles towards the development of advanced CBIs. Chapter 2 presents ICTs (Information and Communication Technologies) that have been currently used to support such requirements, and trends and more advanced ICTs that can be applied in the development of advanced CBIs. Chapters 3 and 4 present the developed CBI, which is called *Plug and Play Horizontal ICT Infrastructure*, or simply *ICT-I*. Chapter 5 gives a general overview of the security framework. Chapter 6 provides an analysis of ICT-I, pointing out its features, innovative aspects and limitations. Chapter 7 gives a final overview of the developed ICT-I.

While this chapter introduces the ICT-I from the conceptual point of view, next book chapter describes its implementation, describing the used ICTs and the developed services.

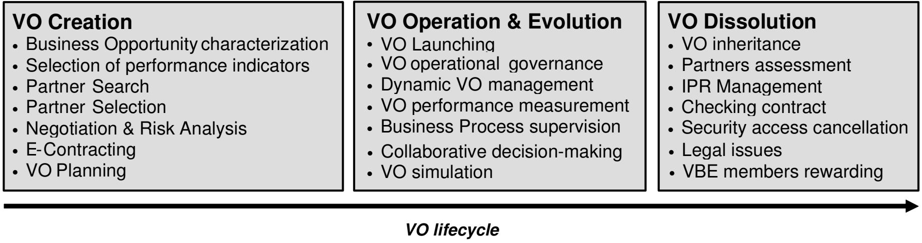
1.1 Functional Requirements for Advanced CBI

CNOs have a different sort of business processes that is not handled by B2B and EIA solutions. Actually, CNO processes complement the processes managed by such solutions. CNO processes use to be interactive/user-centric, asynchronous and not necessarily well structured or defined a priori. The focus is on flexibility and adaptability rather than on execution efficiency. Figure 1 lists just some CNO-related processes (at application level) involved in the life cycle of a CNO of type Virtual Organization (VO), which should then be supported by CBIs.

In order to support such high-level processes at infrastructure level, it can be observed that a CBI for CNOs is much more than supporting the execution of groupware facilities. In fact, a CBI for CNOs should fundamentally provide functionalities associated to five types of elements (Figure 2), enabling:

- *people* to collaborate and negotiate;
- *systems / services* to execute and adapt;
- *knowledge and information* (at *all* levels) to be exchanged and retrieved;
- *computing and human resources* to be discovered and shared;

- *processes* to be interconnected and synchronized.



VO Creation

- Business Opportunity characterization
- Selection of performance indicators
- Partner Search
- Partner Selection
- Negotiation & Risk Analysis
- E-Contracting
- VO Planning

VO Operation & Evolution

- VO Launching
- VO operational governance
- Dynamic VO management
- VO performance measurement
- Business Process supervision
- Collaborative decision-making
- VO simulation

VO Dissolution

- VO inheritance
- Partners assessment
- IPR Management
- Checking contract
- Security access cancellation
- Legal issues
- VBE members rewarding

VO lifecycle

Figure 1 – Example of CNO-related collaborative processes

Security and interoperability are two technological elements that should permeate the CBI, whereas business models can be applied upon the CBI as long as services and resources in general are going to be accessed and also made available to other CNOs' members. Managing this with high efficiency, cleverness and transparency is the challenge to be reached by advanced CBIs.

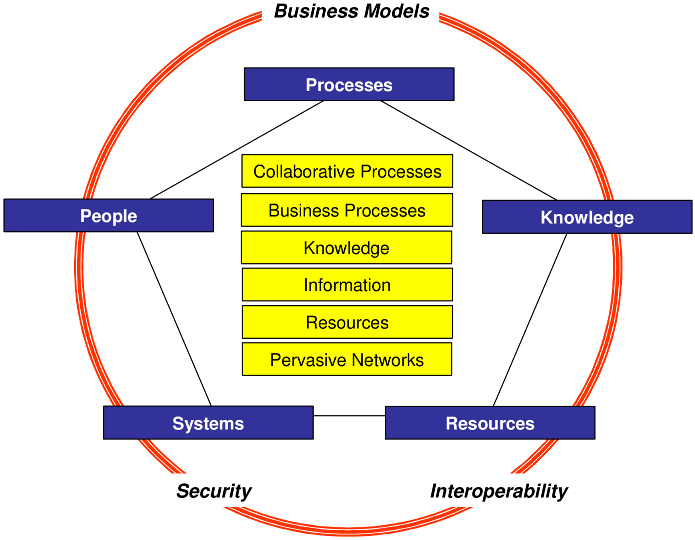


Figure 2 – Requirements for Advanced Collaborative Business Infrastructures

1.2 Technological Requirements for Advanced CBI

A number of business models and ICTs have recently been emerged, and they are being used by some companies already. They represent a clear trend and its impact is tremendous on the way systems have been designed by now. Their consideration in the design of advanced CBIs is of paramount importance as they represent technologies that will increasingly be incorporated into the next generation of eco-systems, which are implemented in a diversity of platforms, equipments and ubiquitous devices.

Figure 3 resumes the characterization of past values and future values in terms of CBIs for CNOs, changing the focus from processing efficiency and full automation, to collaboration flexibility and human intervention. This reflects a scenario where composable and autonomous services of software – deployed in several repositories and seen as utilities – can act with cleverness and flexibility to solve problems and to adapt themselves to changes in the business environment, having the human being as the centre of actions and decisions.

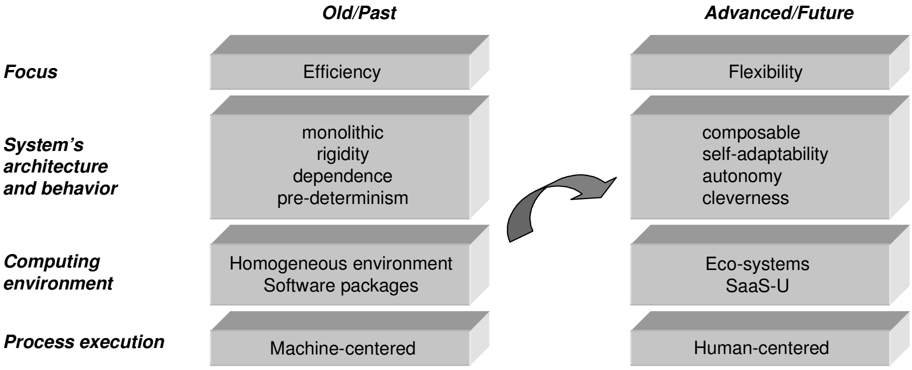


Figure 3 – Shift on the focus of collaborative business ICT infrastructures

1.3 Some Obstacles

Developing a CBI that can be able to cope with all these requirements and that can immediately be adopted by companies is a big challenge. Major obstacles for that involve:

- short ICT life cycle;
- level of companies' preparedness;
- non-alignment of ICT and Business worlds;
- lack of trustworthy environments;
- lack of roadmaps towards Web 2.0 and Enterprise 2.0.

Short ICT life cycle
The fast evolution of ICT technologies with reduced life cycles and the need to cope with technologies with different life cycles and at different stages of the corresponding life cycle has introduced enormous difficulties for developing cost-effective and long-life collaborative tools, especially regarding that in CNO systems of diverse companies should interoperate. However, if on one hand ICT usage is a key enabler element to enhance competitiveness, on the other hand they bring another sort of problems that should be permanently managed by SMEs, which would be difficult regarding their lack of resources and IT skills. Therefore, the project of advanced CBIs should take this into account.

Level of companies' preparedness
A significative underlying motivation of CNO is based on the notion that SMEs can largely benefit from this specially when belonging to strategic alliances like VBE

(Virtual Organizational Breeding Environment (Hamideh and Camarinha-Matos, 2005) and VE (Virtual Enterprise (Goranson, 1999). However, reaching the level of preparedness to indeed work in a CNO is a long and hard way. Hamideh et al., 2004) have depicted the benefits to work collaboratively but also the impact of this in terms of preparedness. The problem is that SMEs have already so many difficulties to have their systems organized, integrated and managed, and expanding this at the inter-enterprise level too is even more complex and demands still more resources and time. Therefore, the project of advanced CBIs should mitigate the usual required efforts spent on this preparedness, namely in terms of systems interoperability and customizations, and of training.

Non-alignment of ICT and Business worlds

A usual complaint from companies and managers about ICTs is that most of them are not only too complex, but they are far from considering the requirements of real business processes. Part of this is caused because ICT people and business people use to work totally separated, leaving the required adaptations and integrations up to software-houses and consultants.

Considering the increasing investments spent with ICT solutions, the fact is that most of SMEs get lost in managing this problem, meaning that they don't know at which extent which ICTs are adding value to businesses nor the medium and long term consequences of their adoption. It can be seen a paradox, but if on one hand ICT is seen as part of the solution to leverage companies competitiveness, on the other hand they face difficulties to find out the most suitable ICTs for them. Actually, the main underlying challenge related to this is to leave managers enthusiastic with ICT in a way they can better reason about how it can bring innovations to their businesses.

It is however important to mention that a new generation of managers is coming, formed by people who were born with Internet and for whom ICT is a routine and not an issue to be feared. They tend to create an additional "entropy wave" to business as they are usually more open-minded and so can introduce deep changes in the traditional way of doing business and so on how business processes should be conducted. This reinforces the need for very flexible and easy-to-use ICT solutions.

Lack of trustworthy environments

Trust building is a cornerstone issue in CNO. When this is to be handled at infrastructure level, it comprises both security and information access. Collaboration should be safe, and authorized partners should only have access to pertinent information that is effectively required for every particular and current business (Mezgar, 2006). This means that there is a life cycle for information access and this should be controlled on the fly, opening the access to the exact and required information for each business as long as transactions are being carried out. All this should be done safely, supported by AAA (*Authorization, Authentication and Accounting*) mechanisms. This is however very much complex to provide, and this lack can mitigate a more intensive and faster adoption of the CNO paradigm by companies. In spite of the existence of several security methods and approaches, there is no solution yet for that envisaged scenario. The security framework developed in ECOLEAD (see Chapter 5) represents an important contribution towards this.

Lack of roadmaps towards Web 2.0 and Enterprise 2.0
Web 2.0 and *Enterprise 2.0* are two relevant movements that have arisen "around" companies and that will impact them deeply, directly or indirectly. Web 2.0 is the business shift in the computer industry caused by the move to the Internet as platform. The idea of Web 2.0 can also relate to a transition of some websites from isolated information silos to interlinked computing platforms that function like locally-available software in the perception of the user. Web 2.0 also includes a social element where users generate and distribute content, often with freedom to share and re-use. In the context of a CBI for CNOs, this imposes important requirements in terms of knowledge search and retrieval as long as the sharing of knowledge and best practices among partners is one of the most powerful evolving mechanisms of a CNO.

Enterprise 2.0 is the general term for the technologies and business practices that liberate the workforce from the constraints of legacy communication and productivity tools like email. It provides business managers with access to the right information at the right time through a web of inter-connected applications, services and devices. Enterprise 2.0 makes accessible the collective intelligence of many, translating to a huge competitive advantage in the form of increased innovation, productivity and agility. Transparency, ubiquity, support for mobility, flexibility, information and knowledge sharing, evolving information systems and folksonomies are features that should be incorporated in advanced systems (Mcafee, 2006).

The problem is that these technologies have been soundly announced as being the future of the companies but there is not any roadmap that helps SMEs to be prepared for that and to benefit from that. Actually, only few companies are able to realize their impact and requirements for their adoption. Advanced CBI for CNOs must hide all this, endowing managers and SMEs with an environment where services, information and knowledge sharing, access and adaptations can be made transparently, seamlessly, intelligently, and in a secure manner.

2. MAIN CONCEPTS AND APPROACHES

This chapter aims at presenting the most important approaches and technologies to deal with the requirements of CBIs for CNOs stressed in chapter 1. It starts mentioning the most important technologies currently being applied, passing by a description about the most relevant trends, and it ends with an explanation of advanced ICTs that can support these trends. In general, each ICT is presented, its basic weaknesses are pointed out, and its usage in a CBI for CNO is identified.

2.1 Current Approaches

Computer Supported Cooperative Work
Computer supported tools for cooperation/collaboration is not a new subject. Since 90ths CSCW (*Computer Supported Cooperative Work*) tools has been a very prominent area providing many tools, both commercial suites and free software packages easily downloaded from Internet. CSCW tools' scope varies quite a lot

from one to another. Some tools only offer specific groupware functionalities whereas others can even treat processes and human interaction in an integrated environment. Despite CSCW advantages, the problem is that this class of systems only gives support for human interaction, when advanced CBI requires much more than this (as already explained).

Workflow systems

Workflow systems are another class of technology that has been growing very much in acceptance by companies nowadays. It is a powerful approach as it allows a tight coordination of flow of activities and can support detailed customizations about the processes to be supervised and executed. They can cover both intra-enterprise and inter-enterprise business processes, besides having capabilities to interact with legacy applications (Chen and Hsu, 2001). Despite its potentialities, the problem is that it works quite well with pre-defined flows of activities associated to each business process. In a CNO scenario, a much higher level of flexibility is necessary during the execution of processes as several collaborative processes are, *per se*, non-structured and/or can't be defined *a priori*. Another drawback is their limitation to work with highly interactive and user-centric approaches, as they were mainly conceived to automate the execution of pre-defined business processes.

Enterprise Application Integration

Although businesses among different companies are generally treated at high-level, it does not mean that "classical" issues are no longer necessary to be dealt with. One of the most relevant issues from the ICT perspective is the access to legacy or corporate systems. In general, these are the systems within which most of the information that flow in the collaborative and B2B transactions comes from. No matter the underlying ICTs used to support this, this issue has been tackled in the scope of the EAI (*Enterprise Application Integration*) area.

EAI can be used for data integration from multiple systems; for process integration in a way to link business processes across applications; for vendor independence in the sense of facilitating the replacement of applications without the need of re-implementing the business rules; and for common front-end of clusters of applications (Lee et al., 2003). In spite of that, current solutions present some limitations when applied to a CNO scenario. One of the major problems is that CNOs require a CBI that supports dynamic and temporary mapping of the information that has to be accessed in every source, in every partners´ database and/or legacy system, for every different business. This also means to manage the fact that each of those sources usually has different formats, semantics, and partners are not necessary previously known to each other. This is very complex as it requires an optimum but flexible design and integration of high-level inter-enterprise business/collaboration processes with (individual) low-level intra-enterprise business/manufacturing processes.

"My" System

Looking at SMEs and the problem of solutions´ customization, the *"my system"* approach is very relevant nowadays. One of the most known cases is *mySAP*[2]. It corresponds to light versions of large packages of software that intends to not only fit the SMEs financial and technical conditions, but also to allow them to only use the most relevant modules' functionalities for their businesses. Adopting this approach, companies keep using large packages anyway, and observations have shown that most of the users of this approach are in fact "large SMEs". Even though, and in what CBIs are concerned, a revision in the literature has revealed the inexistence of something like *"my CBI"*. Besides that, users should either utilize software from the same vendor, or they should learn how to utilize different systems, interfaces and terminologies. Although web-based portal solutions have been used – mostly by large companies – to integrate disparate systems, an ideal solution should provide a CNO with an *integrated* computing environment and supporting infrastructure where intra-enterprise process-based transactions, B2B transactions and inter-enterprises collaborative-based transactions could be carried out seamlessly, no matter which software modules are being used.

Application Service Provider

Another interesting model that has tried to mitigate the impacts of the adoption of modern and more complex systems by companies is the *Application Service Provider (ASP) model* (Dewire, 2002). ASP provides access to applications that are located outside the client environment. In essence, ASPs are a way of companies to outsource some or almost all aspects of their information technology needs, providing a contractual software-based service for hosting, managing, and providing access to an application from a centrally managed facility. For a certain periodical fee, the ASP provides content and other services for users connected through the internet or any other network platform, and the users do not need to be concerned with software versions and upgrades. Although too dependent on the quality of the network and the provider's pricing policy and security infrastructure, ASP became a successful model and it could be useful for SMEs in terms of accessing a CBI remotely. However, companies would keep accessing to and paying for the whole CBI, no matter how much of it would be indeed used, which is not very adequate to CNOs/SMEs.

Component-Based Model

A step forward towards solving the necessity of working with an entire module or system is represented by the *Component-Based Model*. It is a branch of the software engineering discipline, with emphasis on decomposition of the engineered systems into functional or logical components with well-defined interfaces used for communication across the components (Shaw, 1996). Reusability is a key characteristic in this model. A software component should be designed and implemented in a way it can be reused in many different programs. Applying this model at a CBI level has, however, some important restrictions. The most relevant one is the non interoperability among the standard component models, which would mean to force the adoption of an almost proprietary CBI to the CNO members, an unthinkable decision regarding their intrinsic heterogeneity and autonomy.

It is important to point out that a project of a CBI for CNOs has to cope with the need of its fundamental "users", which are the *application clients and users,* and *the developers/providers* of the CBI's functionalities. This means avoiding the common problem in most of infrastructures or development environments, which are either too complex to deploy, to configure and to use by users, or too complex to add new functionalities or changes made by developers.

2.2 Current Trends

Knowledge Search & Sharing
In what *knowledge search* is concerned, Information Retrieval (IR) technique has been the most used supporting approach. In general, its main goal is to provide means for searching information in documents or searching for documents themselves. Traditional implementations, such as *Google*, retrieve documents containing keywords specified in the query. Although such techniques provide some support for semantics, this is not enough to cope with the characteristics of knowledge search in CNOs. From another point of view, one of the trends in the IR area is ontologies, which improves the effectiveness of information search, and helps in knowledge retrieval. However, to deal with CO requirements, a tough reality should be dealt with as partners can be involved in multiple CNOs simultaneously. Each partner has its semantics when publishes information and knowledge, and the involved ontologies are not static, which requires permanent maintenance. This problem is intrinsically complex, but some works have been offering some contributions towards using smart search engines for federated search over highly distributed knowledge sources, as in Tramontin et al. (2007).

Enterprise 2.0 & Web 2.0
As mentioned before, *Enterprise 2.0* and *Web 2.0* will demand another era in terms of information systems and infrastructures. This means that CNOs, as a paradigm vitally linked to computing networks, will need CBIs that are web-driven, using Internet as the core communication mean, allowing an easy and fast configuration, connection and disconnection of partners as long as businesses finish. This is important as traditional infrastructures (or middlewares) are customarily deployed as huge, proprietary and complex packages of software, so going to the opposite direction of CNO needs. In the CNO scenario, where alliances are volatile and the flow of collaboration is sometimes only defined on the fly according to the required (and quite often interactive) business process, more flexible infrastructures are necessary. This means to have something like a *plug and play* infrastructure (Miller et al., 2001), where its existence is even not noticed by users, where interoperability problems are (mostly) hidden, and where is not necessary to have it completely loaded when just few of its functionalities are requested. In resume, this gives rise to lean, on demand and fully standard-based collaborative infrastructures, which allows an “a la carte” and “mouldable” infrastructure for each business.

Service Oriented Architecture
Service Oriented Architecture (SOA) is a more recently paradigm for systems design and integration. It can be defined as an architectural paradigm for components of a system and interactions or patterns between them (Singh et al., 2005). In a SOA-based architecture, all functions – or *services* – are defined using a description language and have evocable interfaces that are called to perform business processes. A *service* is a software element that can both call for other service and be called by another service (www.w3C.org). A service has an interface described in a machine-processable format that is usually platform-independent,

meaning that a client from any device using any operating system in any language can use the service.

From the perspective of a suitable approach for supporting CBIs for CNOs, SOA copes far much with most of the limitations previously mentioned, especially in terms of scalability, modularity and granularity, reusability, independence of platform and technology, and on-demand usability. Despite some open points associated with the implementing technologies so far available to materialize SOA-based systems, SOA is clearly the most relevant current software-engineering approach. According to (Gartner, 2006), 30% of Supply Chain Management (at Intranet level) solutions and 20% at Extranet level already applies SOA-based software, and it is expected that this grows up to 90% by 2010.

Software-as-a-Service & Saas-Utility models
Nowadays the ASP model acquired a more refined vision, where software is no longer seen as a monolithic package to be sold and deployed, but rather as a service to be offered on demand. This has been called the *SaaS* paradigm (*Software-as-a-Service*). In this model, software access is subscription-based, remotely hosted, and delivered over the Internet, without the need of complex implementations and IT infrastructure[3]. This gradual shift in the terminologies is also a direct reflection of the change in the business requirements demanded by customers. The focus of SaaS is more on what the customer wants, rather than what the vendor could give. Anyway, ASP model does not solve some important aspects for CNOs.

SaaS-as-Utility (Saas-U) is seen as an extension of SaaS model. In general, this means to adapt the concept of on-demand application to on-demand service, in a large-scale and ubiquitous environment, where services can be accessed from everywhere and can be composed on the fly to create new applications according to current and variable business rules.

2.3 Advanced Approaches

A number of ICTs has emerged both to offer possible architectural solutions for some of those limitations in the ICTs mentioned above, and to open more advanced perspectives of CBIs for CNOs.

Pervasive computing
Pervasive or Ubiquitous computing integrates computation into the environment or, *computing everywhere*, using “Things That Think” (Singh et al., 2006). It is based on the idea that embedding computation into the distributed environment and everyday objects would enable people to interact with information-processing devices more naturally and casually than they currently do, and in whatever location or circumstance they find themselves (*AAA paradigm – Anywhere, Anytime, Anybody / Any type / Any device*). This is an enabling technology for adaptive infrastructures. Thus, a CBI should act as the “glue” between the needs of a given client application in a given moment and the information pervasive servers can provide in that moment, creating a real-time adaptive and context-aware environment. This technology can allow self-adaptability of advanced CBIs.

Peer-to-Peer
Peer-to-Peer (or just P2P) is a computer network that relies primarily on the

computing power and bandwidth of the participants in the network rather than concentrating it in a relatively low number of servers. Such networks are useful for many purposes. Sharing content files containing audio, video, data or anything in digital format is a very common usage of P2P technology. A pure peer-to-peer network does not have the notion of clients or servers, but only equal *peer* nodes that simultaneously function as both "clients" and "servers" to the other nodes on the network. Therefore, P2P model differs from the client-server model where communication is usually to and from a central server (Parameswaran et al., 2001). Main usages in advanced infrastructures comprise publishing, advertising, searching and exchange / sharing of knowledge, information, applications and services of several types of media from/to heterogeneous & distributed sources (e.g. e-mail, blogs, chats, forums), i.e. among CNO members. This is a technology which can enhance the reliability and hence the efficiency of advanced CBIs.

Grid computing

Grid computing is an infrastructure based on the P2P architecture that allows flexible, secure and coordinated resource sharing among dynamic collections of individuals, resources and organizations. In short, it involves computing resources virtualization. Grid computing offers a model for solving massive computational by making use of the unused resources (*CPU cycles* and/or *disk storage*) of large numbers of disparate computers, often desktop computers (Foster et al., 2001). In a CNO scenario, however, companies are in a collaboration alliance but they usually don’t benefit at all from this. In other words, collaboration can go beyond business opportunities and knowledge: it can also involve computing resources. Therefore, CNO members can rationalize the utilization – and even the purchasing – of computing resources as CNO´s members can share this with each other (Pinheiro and Rabelo, 2005). *Virtualization*, a recent concept in the business arena, can be seen as a facet of this scenario, although its application has been so far used at intra-enterprise level. Grid and virtualization are technologies that can enhance the efficiency and resources rationalization of advanced CBIs.

Multi-agent systems

Multi-agent systems (MAS) is a field of research within the distributed Artificial Intelligence area where a system is composed of one or several (“intelligent computing processors”) - *agents* - that interact with each other (using a high-level protocol) asynchronously and with variable levels of autonomy, with other sources of knowledge and with other systems, to solve complex problems that are intrinsically dynamic and distributed. Depending on the problem requirements, an agent can even move itself to other computers through the network and execute its mission there. This is a technology which can endow some intelligence to an advanced CBI, which can reason about the information gathered via the three technologies mentioned above for clever actions (e.g. services selection based on QoS criteria and information filtering) at infrastructure level (Acampora, 2007).

3. DEVELOPED CBI: THE ECOLEAD ICT-I

After motivating for the need of advanced CBIs for CNOs and stressing the requirements for that, this chapter presents the *concepts* of the CBI developed in the ECOLEAD project. In this project, this CBI is called *ICT-I*, an acronym for “plug and play horizontal ICT infrastructure”. Actually, ICT-I is here described only at conceptual and architectural levels, stressing the devised *Reference Architecture* and the *Reference Services*. The ICT-I itself, derived for the services implemented in ECOLEAD, is detailed presented in the next book chapter.

ICT-I has been designed to cope with most of the identified requirements. Nevertheless, developing a completely transparent, fully interoperable and totally reliable CBI to cope with all CNO requirements is not possible considering the limitations of current ICTs and a good number of related research problems. Moreover, CNO is an emergent area and many related issues are still gaining ground, which means the existence of several open questions. In this sense, the strategy adopted in ICT-I was to design a generic/reference architecture and flexible framework in a way it can evolve as long as newer CNO models and ICTs are introduced and open questions are solved.

ECOLEAD ICT-I intends to cover part of this gap based on the vision of a *plug & play* infrastructure. This means that any VBE/VO/PVC member is provided with adequate tools to be easily *plugged* into the ICT-I / CNO community and to *play* (i.e. to collaborate with other organizations) in a secure, on-demand and pay-per-use way. In order to cope with this need, ICT-I has been fully developed based on open / platform-independent specifications and ICT standards.

Regarding its features and potentialities, ICT-I applies the SOA approach, and *web-services* (WS) is the core technology that has been used to implement ICT-I. An important feature for the desired flexibility and scalability is that ICT-I is not a monolithic piece of software that follows the traditional notion of middleware as a “closed world bus” that allows integration of distributed/heterogeneous parts. Instead, ICT-I is a “pulverized” open bus composed of many distributed services which, on demand and according to the precise needs/services for a given transaction, gives the conditions for CNO members to collaborate and to make businesses. That is why it has been called ICT *infrastructure* and not *middleware*.

ICT-I is a scalable and, to some extent, evolving CBI, as new services can be added and others withdrawn from a logical federation of services providers (including the own CNO members). Different implementations of the same services can co-exist and are accessed following agreed business models, security policies, and according to the current context and performance criteria. ICT-I applies the SaaS-U model. CNO members can have a remote and (mostly) transparent CBI, and they use (and can pay for) only what they need, when they need, without any local deployment. Therefore, ICT-I is *not* a framework for SOA-based developments (like IBM *WebSphere*[4], SAP *NetWeaver*[5] or Oracle *Fusion*[6]), nor an integrated CSCW/Groupware package (like *Lotus*[7] or *PHPCollab*[8]), nor another B2B middleware (like Microsoft *BizTalk*[9]), and not a proprietary services-based platform (like *DBE*[16]). Regarding those SOA frameworks, as they are just frameworks, any of them could be used to develop web-services for CNOs. In ECOLEAD, almost all the developed services have utilized the *AXIS*[10] framework, which is robust, open-source, free and compliant to all the W3C recommendations.

3.1 ICT-I Scope

ICT-I acts as a CNO collaborative bus, allowing different and distributed organizations to interact with each other. As said before, the interaction between CNO members comprehends diverse classes of elements: people, processes, systems, knowledge and resources. ICT-I functionalities are modeled as services (see chapter 4) and high-level applications (ICT-I *clients*) can have access to them via web portals and/or via invoking ICT-I services directly. ICT-I can then be used as the ICT glue to link all those elements, also including CNO members' legacy systems. Figure 4 illustrates this scenario and the ICT-I scope. Services (both from ICT-I and from services-based applications) are registered, deployed and maintained in distributed repositories, which are logically joined in a common area called *Services Federation* (see section 3.4). This distribution is, however, totally transparent to the ICT-I's clients.

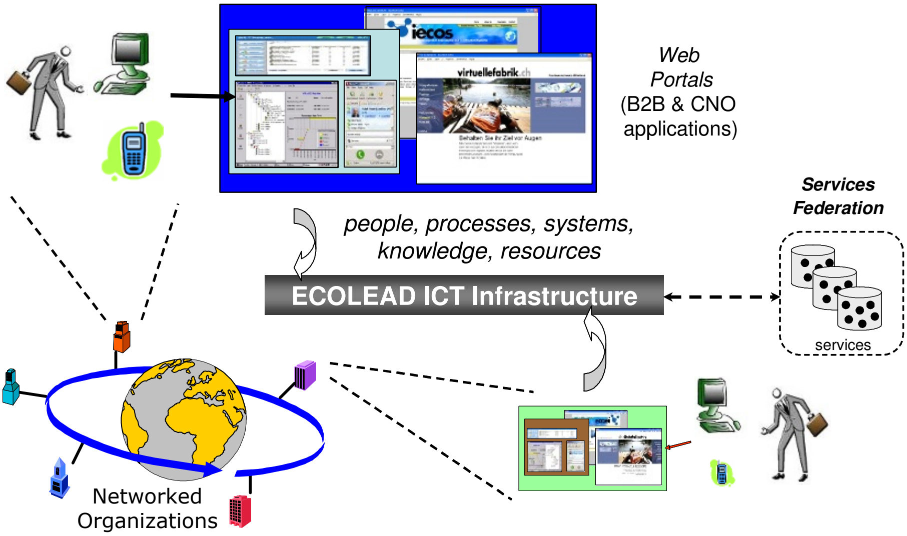


Figure 4 - General ICT-I usage scenario

3.2 Interoperability and Security

Interoperability plays an essential role in any infrastructure where CNO actors and their applications are distributed and heterogeneous. In this context, Interoperability is seen as the ability of a system or a product to work with other systems or products without special effort from the customer or user[11].

Interoperability is a very wide area, comprising since low-level sensors integration till higher levels of inter-organization collaboration. Regarding the core focus of ECOLEAD ICT-I, interoperability aspects are covered only at its essentials, i.e., interoperability issues are tackled by each ICT-I service according to its specific needs, also benefiting from existing software and approaches.

An extremely important enabler for interoperability is the use of standards. Large international initiatives (e.g., OMG, OASIS, W3C and TeleManagement Forum) have been creating specifications with large acceptance by software developers and vendors worldwide. Therefore, to mitigate interoperability problems, the ECOLEAD ICT-I has been fully developed based on ICT standards, independent of computer platforms. Yet, all the current available ICT-I services have been formally specified independent of technology, using the UML methodology, meaning that they can be implemented in any language or environment. However, ICT-I services have been implemented as WS, which is a particular technology. On the other hand, WS have been considered as a standard *de facto* for implementing SOA-based systems, and since recently, newer specifications and initiatives (e.g. WS-I) have overcome initial interoperability problems among different specifications' implementations of WS. An example of this is the WSIF[12], which effectively supports the invocation/interaction among WS deployed in different B2B frameworks.

In the ICT-I design, WSIF is a strategic element to support the ICT-I vision for CNOs. Thanks to it, different CNO members can also share their services among them (following security access rules). This enlarges the collaboration as any company can put available its services, no matter which environment has been used in the implementation of the services. It is to be highlighted that this endows ICT-I services to be integrated to existing organizations' B2B portals, giving to companies a more comprehensive environment where traditional processes and CNO-related supporting services can work seamlessly (Piazza and Rabelo, 2007).

Security is a fundamental element to reinforce trust building in CNO. The security framework that is incorporated in the ICT-I supports authentication, authorization and accounting along the collaborative transactions that are carried out among CNO partners, regarding the different roles and privileges each one has in a CNO. This framework is embedded in the ICT-I. It is flexible and declarative, allowing responsibilities (and eventually delegations) to be dynamically assigned to actors and required security mechanisms settled accordingly (Sowa et al., 2007). It means that the access (their "visibility") to the services (and information) of the federation by users and by other services is prevented considering the CNO actors' privileges. The security framework is described in Chapter 5.

3.3 SaaS-U and related Business Models

Regarding the increasing complexity and powerfulness of B2B frameworks and ERP systems, they have in turn required more powerful computer hosts and sophisticated people to maintain them. Reality has been showing that this is becoming a vicious cycle, which starts to create several difficulties for plenty of CNO members, mostly composed of SMEs. Worse than having to invest to host such systems, companies often use only a very low number of the systems' functionalities but they pay for the whole system, no matter how much or how frequent they are accessed.

ICT-I applies the SaaS-U paradigm (see section 2.2), meaning that its services are accessed remotely, upon request, paid-per-use, based on a contractual software-based service (SLA – service license agreement) for hosting, managing and providing access to its services following QoS levels, no matter where the services providers are and how services have been deployed. This gives rise to several business models to exploit ICT-I, as stressed in Borst et al. (2005), making possible to offer an affordable and 'made to fit' ICT-I for companies.

From the conceptual point of view, this is similar to what *Salesforce.com*'s platform[13] does. The difference is that it offers CRM-related (web) services, which are physically centralized at the Salesforce company. Customers usually pay a fee monthly or pay according to the number of users of a company.

3.4 Services Federation

A fundamental concept in the ECOLEAD ICT-I is the so-called *Services Federation*. A Federation corresponds to groups of devices and software components organized into a single, dynamic distributed system. Members of the federation are assumed to agree on basic notions of trust, administration, identification, and policy. The dynamic nature of a federation of services enables services to be added or withdrawn from a federation at any time according to demand, need, or the changing requirements of the workgroup using it (Sun, 1999).

This concept was adapted to the ICT-I environment, meaning that all CNO-related services are seen as members of a logical entity, the Services Federation. This federation comprises *all* services that can be reached, used and shared among CNO members, involving the ones related to: i) the ICT-I lifecycle; ii) the supporting services for high-level applications (i.e. the ICT-I itself); iii) the CNO life cycle (comprising VBE, PVC and VOM vertical services); and iv) legacy / (intra-organization) (wrapped) systems services. Thus, all existing services can coexist in a virtual logical repository of services and can be accessed transparently and seamlessly according to some rules (see Figure 4).

From the ICT-I point of view, users and applications do not need to know about which services are needed to support a collaborative transaction, where they are, how they should be executed, and which technologies have been used in their implementations. Services are invoked, searched, discovered and properly executed. Providers of such services can be both CNO members and independent software providers/vendors, having their own policies and rules to manage the services repositories. This means that *ICT-I clients* involve not only CNO client applications, but also CNO services providers.

The presented ICT-I is evolving as the Services Federation is a dynamic and self-manageable entity, with new members and services being incorporated to (or modified) and others being withdrawn from it in a transparent way. This also means that a given service may have different implementations available over the network and thanks to smart services search and orchestration mechanisms, the most suitable set of services for a given business transaction can be found out dynamically. This is, however, a challenge issue and some comments about it are given in Section 6.

One of the ICT-I underlying goals is to act as a catalyzer of independent software providers or vendors – private and even from the open source community – that can provide CNO supporting services through the ICT-I. Such community can therefore be seen as a "CNO of services providers", similarly to the Linux community, which add / refine "services" following (standard) rules of quality of software, software development processes (e.g. CMMI), and even the trust level. In this sense, the agreed and involved business models (via SLA) can drive the "quality" of the services or of the repositories a given company can have access to.

The ECOLEAD Services Federation is to be completely open to embrace eco-services for any type of CNO, of domain, with "any" business model (contrarily to *salesforce.com*, which is focused on CRM, it has its particular community of developers, and is not free), using open ICT standards (contrarily to *DBE*, which don't use web-services).

4 ICT-I REFERENCE ARCHITECTURE

In order to provide an open and scalar model, ICT-I has a reference architecture from which instances-of it can be derived for different CNOs. Figure 5 presents the devised *ECOLEAD ICT-I Reference Architecture (ICT-I-RA).* In theory, it comprises all the possible classes of services than can be useful for any kind of CNO. This generalization has considered the three kinds of CNOs tackled in ECOLEAD: VBE, VO and PVC.

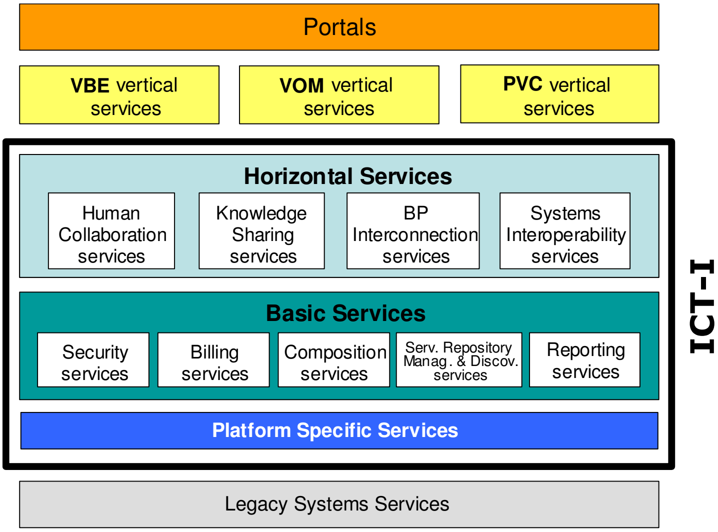


Figure 5 – ICT-I Reference Architecture

4.1 ICT-I Reference Architecture rationale

In the ECOLEAD project, a number of types of CNOs has been comprised, namely VBE, VOM and PVC, for which specific functional needs were identified for each one. Thus, it can be said that such CNOs have *Vertical* needs or, in other words, they require specialized services. On the other hand, they also have some common needs, which help in the execution of any service. For that, ICT-I provides *Horizontal* services, i.e. services independent of any of those three specific applications.

Horizontal services in turn need lower-level services to support their execution, transparently to the application services / CNO actors. These services are seen and called as *Basic* services. They are domain-independent and are essentially used by other services to support the complete and correct execution of a collaborative transaction. Basic services represent the very core of the ICT-I, comprising the discovery, selection and orchestration of services, security, billing and reporting, and some basic interoperability supporting services.

Platform Specific Services is a layer to cope with the fact that, in practice, services (both Basic and Horizontal) require specific tools and/or services when deployed. Therefore, they are intrinsically dependent on the services' implementation.

Legacy system services is another class of reference services. They provide information about activities inside a given company to satisfy vertical services needs. They use to be implemented in heterogeneous platforms and native front-ends, typically representing ERP systems and corporate databases. It shall be pointed out that legacy system services don't belong to ICT-I, but they can belong to the services federation.

As mentioned in section 3.4, when seen as a whole, vertical, horizontal, basic and legacy services compose the Services Federation.

A special and optional element of this architecture is the *Portals*. They act as an integrator front-end (a kind of mega presentation layer, as illustrated in figure 4) to the services themselves, or even to other portals, as a way to invoke services directly by the end-user. Portals are not services.

Per definition, there is not a hierarchy among services. For example, the execution of vertical services requires the combination of services of different nature (considering security aspects, levels of visibility, billing, etc.) no matter the services type (horizontal or basic) and layers they are placed. The effective set of services to be involved and the sequence of their invocation / execution are configured by means of orchestration / composition services, according to the required business processes' rules.

4.2 Derivation of Particular CBIs

A reference architecture is a generic arrangement of modules which represent the most abstract functionalities (or services) that serve as a reference for specializations. In the case of ICT-I-RA, the goal is to be the base for a globally coherent *derivation* of particular ICT-Is (CBIs) for given CNOs. Actually, there are three further stages that have to be passed till building the ICT-I itself.

The first stage of the derivation is the *ECOLEAD ICT-I Reference Framework (ICT-I-RF)*, which is an instance of the ICT-RA. At this stage, the abstract functionalities of ICT-I-RA start to become more concrete and they are already viewed as services. However, they still remain at an abstract level as they are independent of implementation technologies and platforms. This stage and the two others are detailed explained in the next book chapter.

The second stage of the derivation is the *ECOLEAD ICT-I Framework (ICT-I-F)*, which instantiates the ICT-RF's services to particular ICTs. In ECOLEAD, web-services technology and other associated standards (e.g. SOAP and UDDI) have been chosen. Although this particularization, the specification of the services are made in a complete but also abstract way, using the UML standard, which in turn makes the specification of the ICT-I-F still independent of platform. Even though, particular ICT-Is can be further implemented using different technologies (e.g. web-services without SOAP or UDDI) and supporting tools (either open-source or COTS), depending on the envisaged CNO to support.

The third and last stage of such derivation is the implementation and the deployment of the ICT-I's services themselves. As it was already mentioned, this is detailed presented in the next book chapter. Figure 6 illustrates this derivation process in a rough way, picking the case of Human Collaboration services. In the vision applied to it, this is viewed as a CSCW issue. In the derivation done in ECOLEAD, CSCW presents a sort of more specific services, like calendar and file storage. Each of this reference services are completely and formally specified through several UML diagrams, and the services interfaces' description is generated (in the WSDL standard) at the end. In essence, the service name and its WSDL description is the only thing a client application should know to use the ICT-I services.

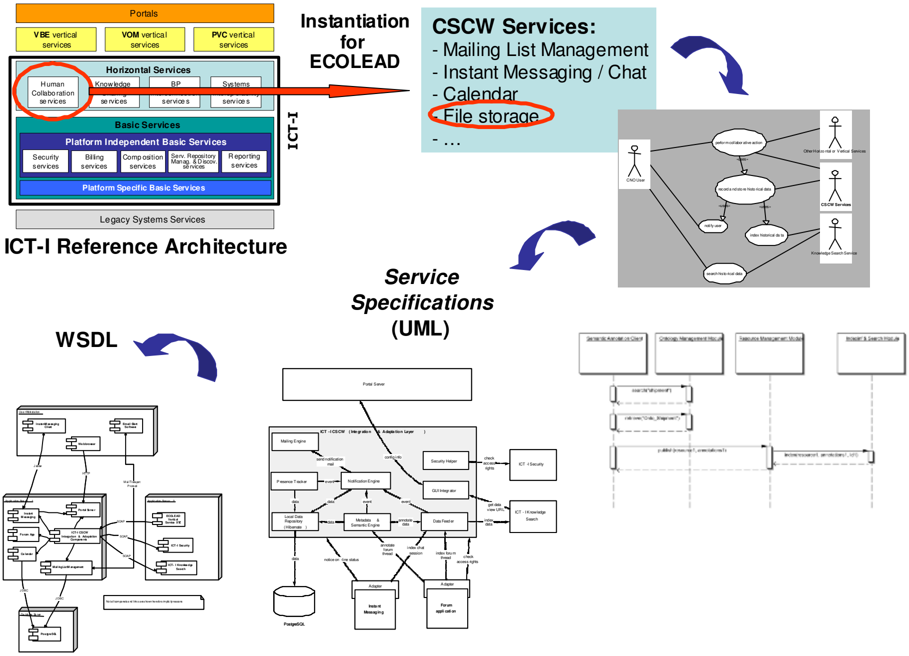


Figure 6 – Derivation Process: from the ICT-I-RA to a CBI

In resume, a CBI derived from the ECOLEAD ICT-I-RA is defined as *an open, distributed, scalable, transparent and security-embedded collaborative service-oriented infrastructure, tailored to support CNOs in the modeling and execution of collaborative tasks, on-demand and paid-per-use*.

4.3 ICT-I Reference Services

This section explains in general the classes of services presented in the ICT-I Reference Architecture.

Horizontal Services

- CNO Actors On-Demand Collaboration Services. For supporting *human collaboration*: mailing, chat, task list, file storage, notification, calendar, wiki, forum, voice and syndication.
- CNO Knowledge Search Services. For supporting *knowledge sharing*, empowering the management of distributed and heterogeneous bodies of knowledge exposed by CNOs. Proper ontology and reconciliation rules have to be used for bridging the semantic gaps among knowledge repositories, allowing seamless retrieval of information.
- Interactive, user-centered BP Management Services. For supporting *business process interconnection*, on top of an existing open-source BPM environment (modeling module and execution engine), ICT-I should provide support to task-oriented, interactive decisional activities to be performed by CNO actors. The forthcoming *BPEL4PEOPLE* standard can also be used for that.
- CNO Data Access Services. For supporting *systems interoperability*, ICT-I needs to offer services to support an easy and secure access to CNO members' databases, which includes the support for defining and configuring them and the information to be shared.

Basic Services

- ICT-I Security Services. These services aim to support confidentiality, integrity, availability and authentication in the communications. This includes the log-in and user management service.
- ICT-I Billing Services. They allow the implementation of different billing models to support the pay-per-use and on-demand service provision.
- ICT-I Services Composition. This service provides facilities to define and execute composed services, preferably using BPEL standard for services composition.
- ICT-I Reporting Services. For supporting the generation of reports to other services (e.g. "detailed billing usage", "services bill summary"), using pre-defined templates in well known formats (e.g. pdf, XML, HTML).
- ICT-I Services Registry and Discovery. For supporting the publishing of the web services in a UDDI repository as well as the search and browsing of services. These services also include the management of the ICT-I life cycle, involving services associated to its deployment, plugging, use, maintenance, unplugging and undeployment.

This description of the horizontal and basic services categories of services is evidently very general since they are detailed described in the next book chapter. The goal here is just to give the core idea of each one, even because the scope and behavior of each service can only be specified when they are designed and implemented.

The derivation process is not a new approach. In the enterprise context, the concept of derivation has been also applied by some more recent relevant initiatives, like VERAM (Zwegers et al., 2003), which acts as a methodology to drive the derivation process of virtual enterprises, from a reference architecture to a particular architecture (therefore, only at abstract level). Another example is ARCON

(Camarinha-Matos and Afsarmanesh, 2006), which extends the virtual enterprise concept to CNOs in a wider reference framework, even though without offering a supporting methodology to derive particular CNOs.

It can be said that ICT-I-RA is positioned at a lower level. It complements those initiatives as it can be seen as a result of an enterprise / CNO derivation process in terms of *supporting infrastructures*. Under this perspective, ICT-I-RA can be used for two different purposes. Firstly, it can be used to derive particular services/functionalities of CBIs for specific CNOs. Secondly, it can be used as a reference, as a “global map”, to guide developments for other CNOs.

5. SECURITY FRAMEWORK

Security is a crucial issue in CNOs. Actually, it is seen as a key enabler element to sustain CNO realization as it requires information and knowledge sharing, as well as very intense electronic (collaborative) transactions among partners. This is even more critic as several sensible information needs to be accessed to guarantee the adequate management of CNOs. In a VBE, for example, partners can share best practices and internal benchmarking. In a VO, partners - especially the VO coordinator - should know the status of production of each member and see their production capacity and scheduling.

Regarding this, most of organizations are very skeptic to share information, and this is worse when there is a need to collaborate with unknown partners. Part of the problem is related to the lack of trust, both between organizations and with their systems. Therefore, and from the technological point of view, security is considered a must to reinforce trust building and, as such, it should be managed properly.

Managing security is very complex. Considering that most of organizations in a CNO are composed of SMEs and that VOs are per definition a unique business, the security mechanisms to support the sharing and information access should be flexible and easily configurable. This allows a quickly setup of the visibility of companies’ information according to each VO needs and of the partners’ roles in every VO. Ideally, this should be dynamically made and adjusted as long as business processes are executed and hence the information access by the involved partners can be controlled accordingly.

However, a number of technical and non technical aspects should be overcome to allow this, like: usual misunderstandings of security management policies by technical staff; a lack of ability to reflect management intentions by IT systems rights (strictly defined static roles); a too long time to transform management decisions into proper configuration of access rights; a too freedom of en-users on their systems environment; hard interoperability problems among different security technologies and mechanisms; and the usual budget restrictions in SMEs. Besides that, most of SMEs have ICT infrastructures that are not fully compliant with security standards and their requirements, and several security tools are not prepared to handle the flexibility and control necessary in CNOs.

Aiming at filling this need, a security framework to cope with CNO requirements has been devised in ECOLEAD[*] (Sowa et al., 2007). In resume, it gives support for the following actions:

- Flexible and easily configurable multi-level security architecture and mechanisms;
- Infrastructure monitoring facilities;
- Dynamic security for allocation and access rights revoking;
- Quality of service and protection.

It can be said that these actions essentially aim to enable the *trust establishment*. These actions are, in fact, used to support security in several concrete CNO-related issues, such as: the management of password, smart card and mobile id logging-in; the management of trust levels; the creation of a new VO; the control of services access; and the control of switching security contexts.

The security framework is embedded in the ECOLEAD ICT-I. It prevents CNO users both from dealing with the usual complexity to deploy security systems, and from knowing security aspects in details. This is achieved via a transparent security environment, facilitating ICT-I acceptance by VBE members and people.

5.1 Legal Issues

Companies are used to follow rules daily. These rules come from the local company's policies, local state laws, national codes of law, and should follow international agreements such as European Commission directives, international pacts, conventions, and treaties. This impacts companies at variable levels as the nature of every business implicates in specific laws that must be followed.

Legal issues have a huge influence on security aspects. The three security pillars - *confidentiality, integrity, and availability* (CIA) - have to be adapted to concrete laws in terms of how systems' functionalities should be executed (Figure 7).

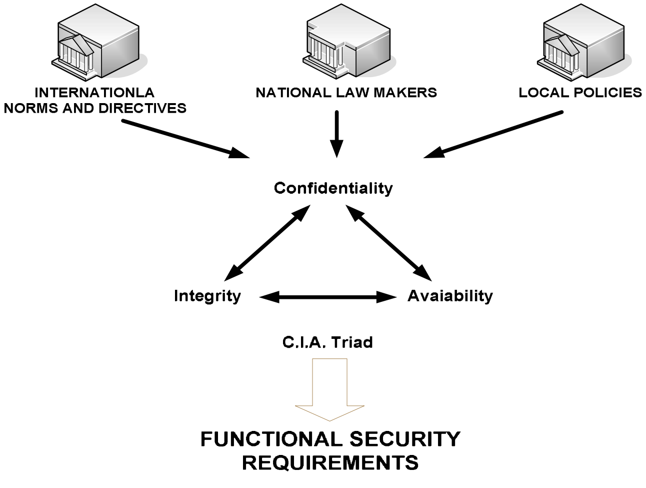


Figure 7 - The impact of legal issues on the security functionalities

[*] Development by COMARCH company.

5.2 A Declarative approach for Security

Security is an issue traditionally considered at coding level when programmers have to implement appropriate mechanisms to check user permissions. Declarative security moves main security aspects to the server level. This avoids applications and web pages to have any code about security into them. This approach is the most important underlying aspect in the ECOLEAD security framework towards security transparency. The declarative approach provides means for selecting the security functionality that is effectively required by a given application / service (Figure 8).

Actually, the ECOLEAD security framework can be viewed as a pool of services that are made available as an API. These services are explicitly chosen at configuration time (e.g. when a VO is created). On the other hand, once a given service is chosen and VO roles are assigned to by the VO manager, the information access rights configuration is dynamically and automatically set up, and the required security mechanisms are used.

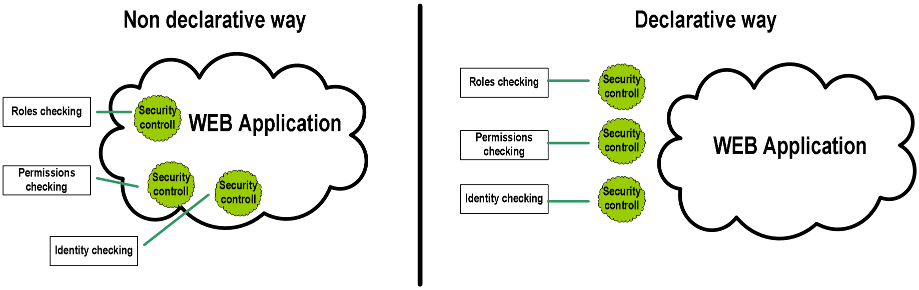


Figure 8 - Declarative security approach

5.3 DRACO Model

The developed security framework supports AAA (*Authorization, Authentication and Accounting*), allowing SMEs to configure the security levels and mechanisms for *each* VO they are involved in. The main element of the security framework is the DRACO (*Dynamic Responsibility Authorization for Collaborative Organizations*) model. DRACO offers flexible ways to define roles in VOs and respective responsibilities (including their delegations) in a way privileges to access information can be dynamically set up. In more concrete terms, DRACO offers:

- Transparent support for web services (ws) security;
- Transparent delegation of end-user identity, starting from the web portal, passing by every intermediary web-service involved in the invocation path, and ending with database (Figure 9);
- Declarative SAML-based authorization at each node of ws-invocation path;
- Guidelines to mitigate the impact of the adoption of the security model in the companies;
- Flexible security for allocation and revoking of access rights;
- Some support for security in mobile computing.

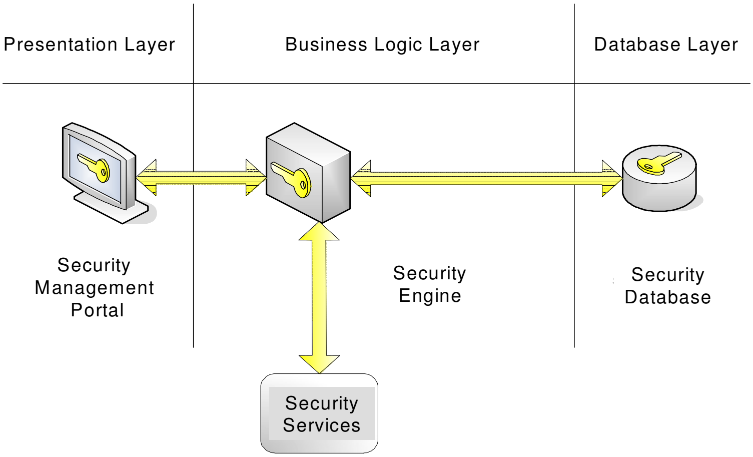


Figure 9 - security management components

Figure 9 also means that some entities (presented in the ECOLEAD vision for CNOs) are directed affected by a security framework. The first one is the end-users, who access services via a web portal and some of them require security (like CSCW tools when some content should be sent out and this should be encrypted). The second one is the companies themselves, i.e. the security required in the transactions involving their systems. The third one is the databases, i.e. how data should be protected, which data may be disclosed, and how security in handled at intra-enterprise level (i.e. internal policies should be coherent with the care a company should take at inter-enterprise level). The last entity is the services providers, which should design their services in a way they are compliant with the required standards and security technologies.

Authentication

DRACO's modules grouped under this services category are responsible for the whole process of getting users' identity, verification of user identity, and the transparent delegation and propagation of the identity to the whole environment.

The concept of transparent delegation is based on the assumption that every single service along the execution path must act in scope of a particular end-user. In order to achieve this, user's identity must be transferred to every involved service. A classical way to support is simply providing the current user's identity in every service call. This approach has some disadvantages, such as the developers must provide user's identity manually every time, and, which is worst, this can be easily tampered. DRACO Security framework provides fully transparent user identity delegation. User's identity is automatically transferred between all components involved in the services execution.

Authorization

DRACO's modules belonging to this service category acts as gatekeepers. Its role is to validate privileges and permissions against the (security) database in a transparent way. At each access point (portal, web service or database) privileges are validated by security filters. User's identity for authorization modules are taken from the authentication modules.

Authorization modules are involved in four situations: every time user invokes a portal's functionality, or a portal invokes a web service, or a web service invokes another web service, or a web service accesses a database.
In the world of DRACO authorization is designed to be completely transparent.

Accounting
DRACO's modules responsible for storing end-user's actions history.

Secure authenticated channels
DRACO's modules responsible for establishing and maintaining encrypted and digitally signed channels between infrastructural components.

These facilities have consequences on some issues and elements that are involved in the security framework and in the services execution. Figure 10 shows this.

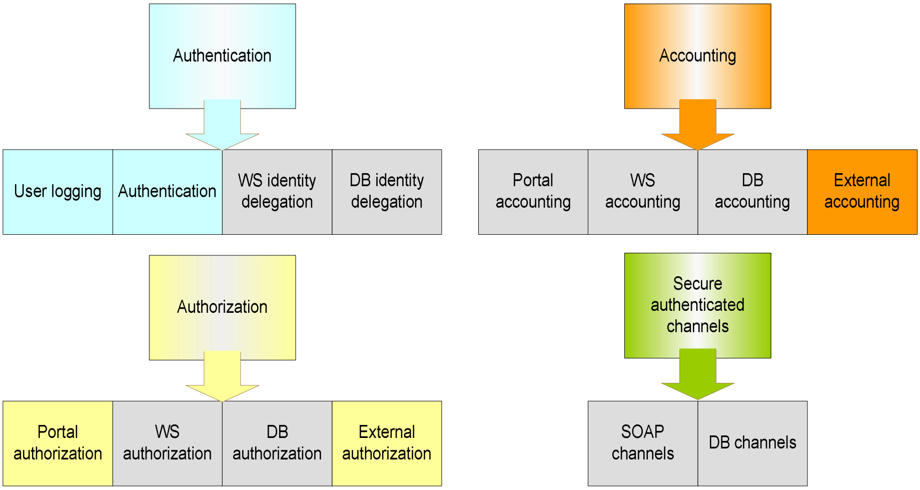
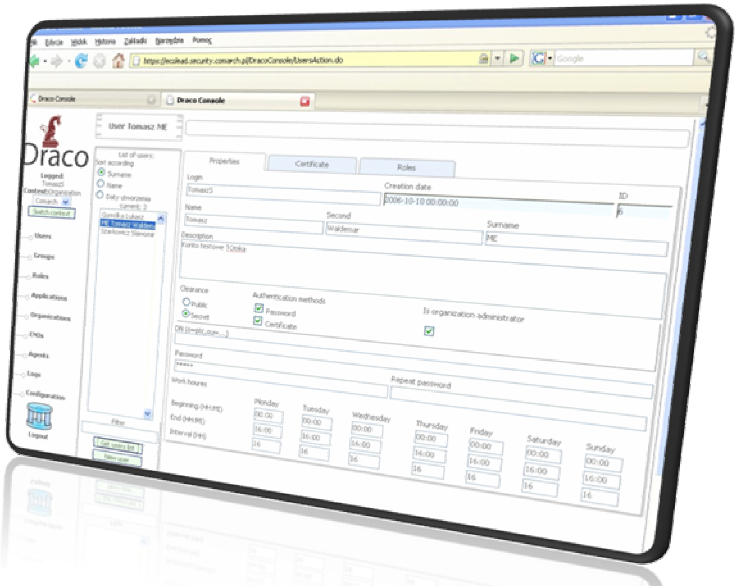


Figure 10 - security management components

Section 5.2 has mentioned that the VO manager (or some authorized person) is responsible for setting up the VO members´ roles and other information. Aiming at facilitating this task, DRACO also provides a user-friendly interface, which is called DRACO's *Console*. Actually, the Console is a service that can be invoked by any application (e.g. VOM system). Figure 11 illustrates one of its graphical interfaces.



User Tomasz ME

List of users:
Sort according
● Surname
○ Name
○ Daty utworzenia
(current: 3)
Gorodka Łukasz
ME Tomasz Waldem
Szatkowicz Sławomir

Login: Tomasz5
Creation date: 2006-10-10 00:00:00
ID: 6
Name: Tomasz
Second: Waldemar
Surname: ME
Description: Konto testowe TOmka

Clearance
○ Public
● Secret

Authentication methods
☑ Password
☑ Certificate

Is organization administrator
☑

DN (o=plc,ou=...)

Password: *****

Repeat password

Work hours

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Beginning (HH:MI)	00:00	00:00	00:00	00:00	00:00	00:00	00:00
End (HH:MI)	16:00	16:00	16:00	16:00	16:00	16:00	16:00
Interval (HH)	16	16	16	16	16	16	16

Figure 11 - security management console

DRACO development has focused on the main issues related to the support of CNO requirements. Other necessary elements of the security framework have benefit from other reference international initiatives in the security area, namely *WS-Federation*[14], *Liberty Alliance*[15] and *WS-Trust*[16].

The main advantage and innovation introduced by DRACO are: *i)* the easy manageable and adjustable access control model based on responsibilities; *ii)* the transparent support for specific needs of evolving and fluctuating structures of VOs (new people and partners can enter in and leave from the structure dynamically); *iii)* the support for most relevant authentication mechanisms (PKI/SPKI, passwords, one-time passwords, biometry); *iv)* the support for multiple forms of responsibility delegation, mapping of responsibilities onto specific application privileges models and; *v)* the application of flexible QoP (quality of protection) policies.

Regarding collaborative processes, four requirements are to be supported by the information security services: *confidentiality, integrity, availability* and *accountability*, no matter if communication is carried out in the traditional client-server model or if mobile codes through the network are involved in. Besides that, it is important to select the suitable mechanisms for every class of transaction as well as for each process phase (normal information exchange phase, contracting and negotiation phase, payment phase, delivery phase, etc.) as security mechanisms use to overhead the network and the client applications themselves.

5.4 Some impacts

In order to attend those requirements, a number of areas (Figure 12) are influenced and hence require a wider vision on how security impacts can be mitigated, regarding that every CNO member is usually very different to each other in terms of systems and security policies.

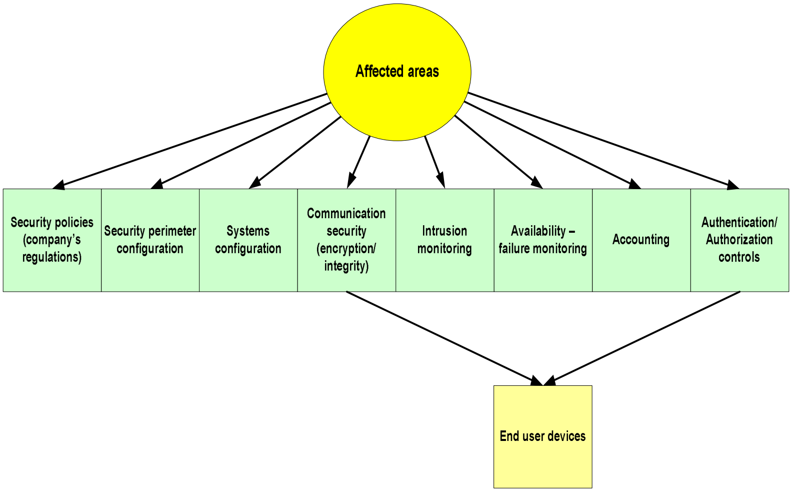

Affected areas
Security policies (company's regulations)
Security perimeter configuration
Systems configuration
Communication security (encryption/ integrity)
Intrusion monitoring
Availability – failure monitoring
Accounting
Authentication/ Authorization controls
End user devices

Figure 12 - Areas affected by security

Another aspect that should also be handled by the security framework is the threats that applications can suffer. In fact, web services bring up a new form of attacks that focuses on exploiting XML. The list of potential new vulnerabilities is manifold:

- Parameter tampering – manipulated XML values are used to conduct fraudulent transactions;
- Coercive parsing – corrupted XML/SOAP messages are used to disrupt and disable unprepared and vulnerable services;
- Recursive payload – deeply nested XML documents are constructed to exhaust computing resources;
- WSDL Scanning – Business APIs are probed for sensitive data and vulnerabilities;
- External Entity Attacks – External references can be made to import certain data;
- SOAP Routing Detours – Messages are redirected to malevolent processing intermediaries;
- SOAP with malicious software – SOAP hides and obscures viruses, spywares, and other similar programs;
- SQL injection into SOAP – SQL code is modified and left undetected because it is embedded in XML;

- WS-Security Spoofing – SOAP security contexts are overridden to gain unauthorized data access.

5.5 Authentication – interoperability between different security technologies

Tools for ICT security are very often considered as weakness and brakes to develop quickly new relationships. Heterogeneity of context, tools and technologies is a real obstacle for SMEs. In CNOs, as companies are heterogeneous, this is much worse and very complex to handle.

In order to enable a secure communication among heterogeneous CNO partners, DRACO solution allows companies in establishing trust relationships with partners even if they use different security technologies/domains (e.g. *SPKI*, *X.509* and *Kerberos*). In general terms, this is achieved by means of the generation and assignment of a generic "security token" to each partner. Figure 13 illustrates a CNO (VO) where the organizations are grouped according to security technologies. When a VO is going to be created as an answer to a given collaboration opportunity, this interoperation problem should be transparently resolved.

In the scenario depicted in the figure below, the problem is that each partner has a different security technology. The VO Manager only supports X.509, which means that all partners would have to use X.509tokens/certificates to communicate with it. In addition, these tokens should be issued by an organization that the VO Manager trusts. The main difficulties in this scenario are: (1) locating this organizations that the VO Manager trusts; and (2) defining how the tokens/certificates will be issued.

In the developed security framework, the infrastructure to support the VO is fully based on web services and on its security specifications (such as *WS-Trust* and *Security Assertions Markup Language - SAML*). WS-Trust defines a *Security Token Service (STS)*, which is responsible for issuing standard security tokens that should be understood by all CNO participants. Security tokens are represented by *SAML* assertions and used to establish the trust relationships among the VO partners. Access rights or roles to each partner in the VO are dynamically assigned by the VO Manager, managed by DRACO, and expressed in SAML assertions. This means that the security technologies present are not important to the communications within a VO, as the only security token used in all communications will be the SAML tokens issued by DRACO.

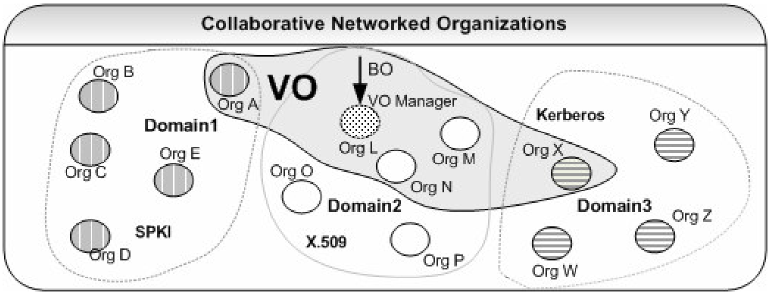


Figure 13 - A VO immersed in different security domains.

5.6 Affected Entities and general assessment

The use of the developed security framework affects three categories of entities associated to a CNO and to the ICT-I: the CNO users, CNO actors, and the CNO services providers.

CNO's users are the people involved in VO activities and who accesses portals and the available high-level CNO-related applications (e.g. VBE management portal, VO management portal, etc.). Impact from their perspective is the necessity to use some specialized security tools (for instance, e-mail message encryption), which can be not that easy to be understood by users. This can also comprise situations where external tools are invoked but they are not fully integrated with ECOLEAD portals, which can break the security chain. Another important factor, especially when considering access to the portal via mobile devices, is the limited capabilities (in terms of memory and processing power) and lack of expandability of some devices, which would then require additional and advanced functionalities that would not be available.

CNO's actors are the organizations participating in a VBE or VO, for example. As it was already mentioned, organizations are usually highly heterogeneous in terms ICTs and security technologies, and most of SMEs are not aware about how important is to adopt ICT standards. This heterogeneity brings hard interoperability problems and can put down a long effort in the changing of the organizations' mentality to work as a CNO. Although DRACO has provided some solutions for that as well as the adopted approach had mitigated the impacts of the introduction of the security framework in the companies, several issues are still unsolved. On one hand this means that CNO members should be aware about this to do not overestimate the level of possible transparency in the systems and ICT-I. On the other hand, they can try to take this interoperability issue into account when designing their systems' architecture and selecting software products or services.

CNO's Software Providers are companies which develops applications and services for CNOs. Similarly to CNO's companies, these providers are usually heterogeneous too in terms of ICTs used, standardization awareness, quality of development process, etc. No matter if they are the own members of a CNO or they are external companies (outsourcing model), they should consider the requirements stressed above so that their services can be compatible with the ICTs used in ECOLEAD, ICT-I and security framework.

The negative impact on the organization environment is potentially high. New forms of attacks and more open networks must lead to paying significantly more attention to operating systems' configuration. This means that more resources should be put on configuration checking, operating systems updating, systems parameters verification, systems hardening, etc.. Another aspect is that the security in every application must be verified and tested in order to eliminate the most common security problems.

In terms of support to mobile devices, it is important to point out their limitations (memory, processing power, modularity) and different built-in features. For exploiting the whole scope of security services (encryption, integrity, methods of authentication) some additional modules must be provided for the above devices.

The Security Framework is not locally deployed. Following the same SaaS-U principles adopted in the ICT-I, security services and facilities are used on demand.

6. GENERAL ASSESSMENT

This chapter provides a general assessment about the ECOLEAD ICT-I, positioning it against other relevant initiatives, highlighting its innovative aspects, and pointing out some of the main open issues and foreseen challenges.

6.1 ICT-I Positioning against other initiatives

ICT-I-RA is evidently not the only one which tries to generalize concepts and services related to enterprises operation. Figure 14 shows the positioning of ICT-I-RA against other reference initiatives. In order to facilitate the comprehension, three different perspectives have been considered, i.e. where these reference initiatives are placed from the process, reference interoperation and Software-as-a-Service (SaaS) paradigm points of view.

From the *process* perspective, ICT-I-RA is placed at a CNO / collaborative level. Any other RA has been found out in the literature which is placed at this level too. At intra-enterprise level there is other RAs, like the *IBM Reference Architecture*, which a direct analogy can be established with if compared to ICT-I-RA: business layer with vertical services, human & process integration with horizontal services, process automation with basic services, and resources virtualization with legacy and basic services. As they are at different business layers, these two RAs complement to each other.

From the *interoperation* perspective, ATHENA project can be considered as the most relevant recent initiative to propose interoperability solution for B2B & at intra-enterprise level. Its reference architecture comprises enterprise models, processes, general services, and information and data that should flow across processes. There are other RAs for interoperability, which cope with other dimensions of interoperability, such as for grid computing and mobile computing. ICT-I-RA does not focus on interoperability. Its services make use of RAs that deal with interoperability according to the approach used in services derivation, implementation and deployment.

From the SaaS perspective, NESSI-RA[17] can be considered one of the most relevant ones. In resume, NESSI sees services as entities that sustain business processes, which should be composed to establish the correct set and flow of services and their execution, that exist and needs to be organized, and that require a computing infrastructure to run. Projects like ECOLEAD, DBE[18] and ABILITIES[19] offer some support just for the three first facets.

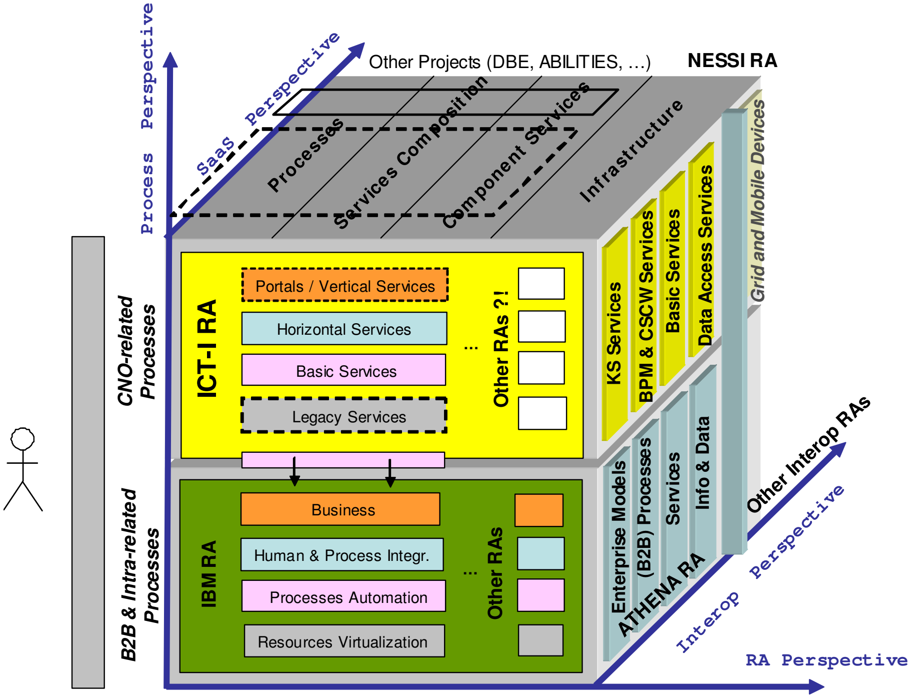


Figure 14 – Positioning of ICT-I-RA against other initiatives

6.2 Innovative Features

Supporting CNOs imply in a different set of functionalities, meaning that ICT-I complements B2B functionalities as well as it adapts and integrates traditional groupware functionalities to a CNO environment. Thanks to the ICT-I framework flexibility and strong utilization of standards, all these functionalities can be integrated in the same computing working environment so that users do not need to see them as separate systems.

From the technological point of view and following current trends, ECOLEAD ICT-I has as main features:

- It is a web/SOA/standard-based integrated platform devoted to CNOs, meaning that users should only have a browser and internet access. No local deployments;
- Suitable and feasible for SMEs;
- It is open and flexible to embrace new services without any interference in the use of the infrastructure, also meaning that ICT-I can intrinsically evolve;
- Services are accessed on demand (SaaS-U paradigm) and can be found out in a clever way, according to the business process flow. This means having almost an ‘a la carte’ environment to fit each organization’s needs.
- Services are paid per use, respecting variable and flexible business models;
- (Some) Services can also be accessed through mobile devices.

- Services and data access are dynamically controlled by a flexible security system.

Regarding its CNO orientation and other features stressed along the paper, it is believed that ICT-I is unique and it clearly goes towards supporting several requirements of Web 2.0 and Enterprise 2.0. Besides that, its conception and features are in line with a number of relevant initiatives, like NESSI and ATHENA.

6.3 Challenges & Impacts

Although a CBI based on the ICT-I RA had been successfully derived for the CNOs and pilots involved in the ECOLEAD project, it can't be said it is finished. Actually, besides the development of other services of the ICT-RF (see next book chapter), there are some open issues and challenges to be faced, some of them associated to the decisions taken in its design. Some of them are generally mentioned below.

Web-service technology, despite its potentialities and increasing acceptance, has some drawbacks (e.g., it is stateless) that should be managed depending on the desired business process's behavior. Dealing with large-scale fault-tolerance platforms is still an open and very complex topic of research so it is expected that future outcomes of this can be incorporated in the ICT-I. Another complex issue is the management of the services federation. Each service provider can determine its own operational and security rules besides having different levels of computing infrastructures to run services, which can create serious troubles and to lead to other class of interoperability problems when several providers were established.

Moreover, the operational policies should deal with the different life cycles of each service that is made available, which is also complex. Services should be easily discovered and immediately integrated/bound to workflow or orchestration systems mechanisms, but this bumps into the different ways and semantics the diverse providers have registered the services, on how the services interfaces (WSDL) are expressed, and if context awareness has to be considered.

All these difficulties represent challenges in the web-related community in spite of several ongoing works. Two interesting research projects that can be mentioned and that are dealing with some of those problems are DBE and ABILITIES, but their results are still not at a level for being now used. These problems are essentially related to the *technological* perspective of the difficulties and impacts the adoption of the CNO paradigm by companies and the use of such kind of CBI to support their collaboration tends to provoke. As mentioned in the introduction, other perspectives, e.g. organizational, cultural, financial, among others are also extremely relevant and must be dealt with properly for the successful realization of the CNO paradigm. These perspectives are, however, out of scope of this book chapter.

7. CONCLUSIONS

This chapter presented an overview of the main issues that advanced collaborative business infrastructures (CBI) for CNOs should consider, and the one developed in the ECOLEAD project (called *ICT-I*), which corresponds to a CBI derived from the *ECOLEAD ICT-I Reference Architecture.*

ICT-I has been conceived based on the service oriented architecture paradigm / web-services technology, providing organizations with a transparent (mostly), platform-independent, easy deployable and configurable, secure-embedded, lean, distributed, scalable, on-demand and pay-per-use CBI. The presented features and its focus on CNO make it somehow unique.

It has been validated within ECOLEAD, close to the 20 developers and 9 pilots of the project, considering three types of CNOs (i.e. ICT-I "clients"): Virtual Organization Breeding Environments (VBE), Virtual Enterprises / Organizations / Teams (VE/VO/VT) and Professional Virtual Communities (PVC).

ICT-I doesn't aim to compete with B2B framework or EAI solutions. Instead, it aims to complement them regarding that supporting CNOs imply in a different set of functionalities, including an adaptation of traditional groupware functionalities to a CNO environment. Interoperability is not its focus, being restricted to the requirements of each service when they are implemented.

The concept of Services Federation is extremely powerful as it allows a seamlessly access of any service of the federation, no matter where services are and how they were deployed. Besides that, depending on the richness of the services and involved business models, several equivalent services can co-exist and can be selected according to performance criteria, business context and business process alignment. New services can be incorporated to the Federation along its life cycle and withdrawn from it, transparently to the clients. However, tough issues should be more researched in order to realize the full concept of Federation. Examples of this include the conception of supporting services for the management of the services federation's life cycle, and of advanced searching mechanisms and semantic-driven services selection and composition over large-scale services repositories.

Although thought as generic as possible, ICT-I-RA can naturally evolve as CNO area is only now gaining maturity. So it is expected that new services, concepts, etc., have to be contemplated by it and in the derivation process, as long as new achievements – of any nature – are made available.

Acknowledgments
This work was mostly supported by the European Commission under the project IST FP-6 IP ECOLEAD project (www.ecolead.org). The Brazilian participation was also supported by the Brazilian Council for Research and Scientific Development – CNPq (www.cnpq.br) in the scope of IFM project (www.ifm.org.br).

8. REFERENCES

1. Acampora, G.; Loia, V. - A Proposal of an Open Ubiquitous Fuzzy Computing System for Ambient Intelligence, in Computational Intelligence for Agent-based Systems, Eds. Raymond Lee and Cincenzo Loia, Springer, pp.1-26, 2007.
2. Afsarmanesh, H.; Camarinha-Matos, L.M. - A Framework for Management of Virtual Organization Breeding Environments. Proceedings PRO-VE'2005 – 6th IFIP Working Conference on Virtual Enterprises, Kluwer Acad. Pub., pp. 35-48, 2005.
3. Afsarmanesh, H.; Marik, V.; Camarinha-Matos, L.M. - Challenges of Collaborative Networks in Europe, in Collaborative Networked Organizations – a research agenda for emerging business models, Ed.s Luis M. Camarinha-Matos and Hamideh Afsarmanesh, Kluwer Acad. Pub., pp. 77-90, 2004.
4. Borst, I.; Arana, C.; Crave, S.; Galeano, N., Technical Report (Deliverable) D62.2 ICT-I Business Models, October 2005.

5. Camarinha-Matos, L. M.; Afsarmanesh, H. - Towards Next Business Models. In Collaborative Networked Organizations: a research agenda for emerging business models, Kluwer Academic Publishers, pp. 3-6, 2004.
6. Camarinha-Matos, L. M.; Afsarmanesh, H. - A Modeling Framework for Collaborative Networked Organizations, in Proceedings PRO-VE'2006 – 7th IFIP Working Conference on Virtual Enterprises, Springer, pp. 3-14, 2006.
7. Chen, Q.; Hsu, M. - Inter-enterprise collaborative business process management. Proc. 17th IEEE Int. Conf. on Data Engineering, pp.253-260, 2001.
8. Dewire, D. T., Application Service Providers - Enterprise Systems Integration, 2nd Edition, pag.449-457. Auerbach Publications, 2002.
9. Foster, I., Kesselman, C.; Nick, J.; Tuecke, S. - The Anatomy of the Grid: Enabling Scalable Virtual Organizations, in Int. J. of High-Performance Computing Applications, pp.200-222, 2001.
10. Goranson, T. - The Agile Virtual Enterprise – Cases, Metrics, Tools, Quorum Books, USA, 1999.
11. Lee, J.; Siau, K.; Hong, S. - Enterprise integration with ERP and EAI, ACM, New York, USA, Vol 46, Issue 2, pp. 54-60, 2003.
12. Mezgar, I. - Trust Building for Enhancing Collaboration in Virtual Organizations, in Proceedings PRO-VE'2006 – 7th IFIP Working Conference on Virtual Enterprises, Springer, pp. 173-180, 2006.
13. Mcafee, A.P. - Enterprise 2.0: the dawn of emergent collaboration, in IEEE Engineering Management Review, Vol 34, Issue 3, page 38, 2006.
14. Parameswaran, M.; Susarla, A.; Whinston, A. - P2P Networking: An Information-Sharing Alternative, in IEEE Computing Practices, pp.31-38, 2001.
15. Pinheiro, F.; Rabelo, R. J. Experiments on Grid Computing for VE-related Applications, in Proceedings PRO-VE'2005 – 6th IFIP Working Conference on Virtual Enterprises, Kluwer Acad. Pub., pp 483-492, 2005.
16. Piazza, A.; Rabelo, R. J. An Approach for Seamlessly Interoperation among heterogeneous web services-based B2B Frameworks [in Portuguese], in Proceedings 8th Brazilian Symposium on Intelligent Automation, pp. 451-458, 2007.
17. Shaw, M.; D. Garlan - *Software Architecture: Perspectives on an Emerging Discipline*. Prentice Hall, Upper Saddle River, NJ, USA, 1996.
18. Singh, M.; Huhns, M.; Service Oriented Computing -Semantics, Processes, Agents, Wiley, 2005.
19. Singh, S.; Puradkar, S.; Lee, Y. Ubiquitous computing: connecting Pervasive computing through Semantic Web, in Int. Journal on Information Systems and E-Business Management, Springer, Vol. 4, N4, pp. 421-439, 2006.
20. Sowa, G.; Sniezynski, T. - Technical Report (Deliverable) D64.1b – Configurable multi-level security architecture for CNOs, in www.ecolead.org, 2007.
21. SUN - JINI Technology Architectural Overview, http://www.sun.com/jini/whitepapers/architecture.html, Jan 1999, in 30/08/2005.
22. Tramontin, R.; Rabelo, R. J. - A Knowledge Search Framework for Collaborative Networks, in Proceedings PRO-VE'2007 – 8th IFIP Working Conference on Virtual Enterprises, Springer, pp. 573-582, 2007.
23. Zwegers, A.; Tolle, M.; Vesterager, J. - VERAM: Virtual Enterprise Reference Architecture and Methodology, in Global Engineering and Manufacturing in Enterprise Networks (GLOBEMEN), pp17-38, 2003.

[1] www.eubusiness.com/topics/SMEs

[2] www.sap.com/solutions

[3] http://www-304.ibm.com/jct09002c/isv/marketing/saas/index.html

[4] www-306.ibm.com/software/websphere/

[5] http://www.sap.com/platform/netweaver

[6] http://www.oracle.com/applications/fusion.html

[7] www.ibm.com/developerworks/lotus/products/notesdomino/

[8] http://sourceforge.net/projects/phpcollab/

[9] www.microsoft.com/biztalk/default.mspx

[10] ws.apache.org/axis/

[11] www.atena-ip.org

[12] http://ws.apache.org/wsif

[13] www.salesforce.com

[14] http://www.ibm.com/developerworks/library/specification/ws-fed

[15] http://www.projectliberty.org

[16] http://docs.oasis-open.org/ws-sx/ws-trust/v1.3/ws-trust.html

[17] NESSI Strategic Research Agenda - Framing the future of the Service Oriented Economy. Version 2006-2-13 (http://www.nessi-europe.com/documents/NESSI_SRA_VOL_1_20060213.pdf); ICT for Enterprise Networking (http://cordis.europa.eu/ist/directorate_d/en_intro.htm).

[18] www.digital-ecosystem.org

[19] http://services. txt.it/abilities