FP6 IST STREP PROJECT N° FP6-027 083

FLUID-WIN

Finance, Logistic and Production Integration Domain by Web-based Interaction Network

Deliverable D24

Requirements to Standards

Release 1

Dissemination Level: Public

027 083

Title	:	**Deliverable D24** **Requirements to Standards**
Document type	:	Deliverable
WP/Task	:	WP 7 – IST Research Cooperation
Version	:	1
Date		12.01.2009
Status	:	Final version

Organisation	:	TUK, Fraunhofer IPK, Regens, Joinet, AL
Authors	:	Heiko Weinaug, Markus Rabe, Bruno Mussini, Michele Zanet, Jozef Bucko, Peter Mihok, Martin Vejacka

Distribution	:	Partners, CEC, Review

Purpose of Document	:	Formal project deliverable

Document history	:	-

1 Management Summary

This document summarizes experiences collected during the FLUID-WIN project with respect to the usage of standards and gaps identified between the requirements in the project and these standards. The document has four major parts:

- Standard relationship with respect to models (e.g. SCOR); responsible: IPK (with specific support on request from Joinet, AL and Régens)
- Standard relationship with respect to message exchange and other IT aspects (e.g. UBL); responsible Joinet with major support from Régens and AL
- Standard relationship with respect to authorization; responsible TUK (with support from other R&D partners on request)
- Standard relationship with respect to the platform and process evaluation

As the result of this investigation, there is no urgent need for further standardisation detected by the project, except in the security and trust domain. In the latter, only the need for such standard is emphasized, while the project has no specific demands on the details of such standard.

In the business process modelling domain as well as for the technological standards, the existing standards have been found not sufficient to cover the modelling elements required.

With respect to business process modelling (BPM), the IEM worked fine, but problems are clearly foreseen if interoperability would have been requested among the companies in terms of BPM. In “real life” the existence of models in other representations than IEM are very likely.

With respect to the message exchange, the best-fitting approaches xCBL and UBL lack information that inevitably has to be exchanged for the FLUID-WIN purposes. The list of gaps can be helpful as one important input to future extensions. However, the project experience will not deliver sufficient generality to claim for a specific extension of the standard.

Information Society
027 083

FLUID-WIN

2 Contents

3 Introduction

The term standardisation can have several meanings depending on its context. A common use of the word “standard” implies that it is a universally agreed-upon set of guidelines. However, the plurality of standard-issuing organizations indicates that a document purporting to be a "standard" does not necessarily have the support of many parties. As Grace Hopper said (Billings, Ch. W. 1989), "The wonderful thing about standards is that there are so many of them to choose from".

In the context of business information exchanges, standardisation refers to the process of developing data exchange standards for specific business processes using specific syntaxes. These standards are usually developed in voluntary consensus standards bodies such as the United Nations Center for Trade Facilitation and Electronic Business (UN/CEFACT), the World Wide Web Consortium W3C, and the Organization for the Advancement of Structured Information Standards (OASIS).

Standards can be “de facto”, which means they are followed for convenience, or they can be “de jure”, which means they are used because of (more or less) legally binding contracts and documents. Government agencies often have to follow standards issued by official standardisation organizations. Following such standards can also be a prerequisite for doing business on certain markets, with certain companies, or within certain consortia. Major Web standards, in the broader sense, include:

- Recommendations published by the World Wide Web Consortium (W3C)
- Internet standard (STD) documents published by the Internet Engineering Task Force (IETF)
- Request for Comments (RFC) documents published by the Internet Engineering Task Force
- Standards published by the International Organization for Standardization (ISO)
- Standards published by Ecma International (formerly ECMA)
- The Unicode Standard and various Unicode Technical Reports (UTRs) published by the Unicode Consortium
- Name and number registries maintained by the Internet Assigned Numbers Authority (IANA)

The scope of this document is:

- to identify standardisation and pre-normative activities within the framework of FLUID-WIN project
- to identify the areas and domains of the standardisation activities
- to promote standards based on the FLUID-WIN project research and experiences.

We will answer the following questions:

- What standards related to what areas are being either used or being developed as new standards?
- What standards in what research areas are lacking?
- Do we need some enhancement of the existing standards?

The FLUID-WIN Project covers the material flow among the European supply network as well as the financial flow associated with this supply. The modellers that have been developed in the course of the FLUID-WIN project allow for customisation of these workflows. The new process model includes:

- Standard processes at the Platform, which are not changed for the single member (of course, new members’ requirements can be adopted in the regular process of ongoing developments)
- Interfaces, which are specified publicly and supported by guidelines and examples.
- Template processes at the members, which are different for the sectors (manufacturing, logistics, finance) and which can be freely used, combined or amended by the members, as long as they follow the guidelines and provide correct support to the interfaces.

In order to reach these goals, this document is structured into two major parts:

- Standards that have been considered, and their use for the project
- Identified gaps with respect to these standards

4 Standards Considered and Selected for the FLUID-WIN Project

The complexity of the project required to consider standards for different classes:

- Business and Process modelling, for defining the new FLUID-WIN Model (example: SCORE)
- Technological standards, for defining how to exchange data among the different components of the FLUID-WIN Platform and among the FLUID-WIN platform and the gateways (Web services, SOAP) and corresponding data modelling, for defining the content of data exchanged (example: XML)
- Security and trust mechanisms
- Standards for the platform and process evaluation

In the following a summary referred to the different classes is presented. It is partially based on the results described in a previous non-public report (deliverable D12). In each of the four classes one of the standards has been selected.

4.1 Business Process Modelling

4.1.1 Enterprise Modelling

In order to follow the requirements of a process oriented modelling procedure, the Integrated Enterprise Modelling (IEM) Method (Mertins and Jochem 1999) was chosen as the basic modelling technique, with the tool MO²GO for its efficient use. This method is very flexible, and the tool supports the application specific definition of resource sets, evaluation schemes etc.. Furthermore, through the object oriented approach of the IEM the use of reference classes is very efficient, simplifying the task of defining common terms, structures and attributes.

The IEM provides Interoperability support by being compliant with the relevant standards for modelling (ISO 19440) as well for transforming model content to third party tools (BPDM, XMI, STEP, EPC).

With respect to modelling constructs, the ISO 19440 and specifically IEM have proven sufficient for all business process modelling requirements that occurred during the FLUID-WIN project. However, IEM does not directly provide guidance for interoperability modelling, which is therefore discussed in the next section, separately.

4.1.2 Interoperability Modelling

The most crucial challenge is the handling of the business-to-business-net approach in different implementation levels. In order to structure the modelling requirements as well as the modelling itself, a framework for modelling cross-organisational business (CBP) processes from the ATHENA research project is used. The CBP framework was developed to provide modelling support for the business and technical level as well as for the transformation to executable models (Greiner et al. 2007, Mylopoulos and Papazoglou 2009). The CBP framework consists of two dimensions (figure 1):

1. Modelling level dimension, related to business, technical and execution processes, which each address different stakeholders.
2. Abstraction layer dimension, defining the target-specific aggregation and filtering of information, which allows the selective nondisclosure of company-internal information while offering to expose CBP-relevant information to partners.

The modelling level dimension incorporates three further modelling levels, as shown in figure 1:

The *Business level* represents the business view on the cooperation and describes the interaction of the partners in their cross-organizational business process. The CBPs modelled on this level allow the analysis of business aspects, like involved partners and their responsibilities. At this level, the FLUID-WIN B2(B2B) Business Process Model covers the processes of the

- business-to-business collaboration within a supply chain (manufacturing)
- business interaction with logistic service providers
- business interaction with financial service providers
- support and functionality of the new integrative services of the FLUID-WIN Platform and their relations among each other

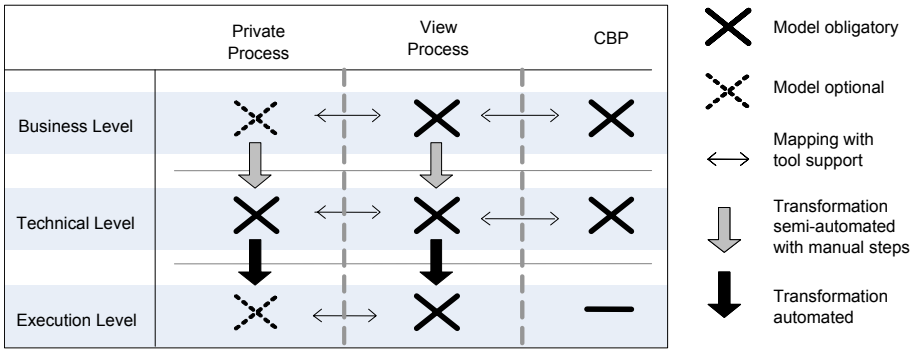

Fig. 1: *Cross-organisational Business Process (CBP) Framework (Greiner and Jäkel 2007)*

The *Technical level* represents the complete CPB control including the message exchange. Thereby, different task types can be distinguished: those which are executable by IT systems and those that are executed, manually. However, the control flow and the message exchange are specified independently on a concrete execution platform.

On the *Execution level* the CBP is modelled in the modelling language of a concrete business process engine, e.g. a model based on the Business Process Execution Language (BPEL). It is extended with platform-specific interaction information, e.g. the concrete message formats sent or received during CBP execution or the specification of particular data sources providing data during process execution.

The abstraction layer dimension is based on the concept of process views on the range between the private processes and the CBP model, as proposed by Schulz and Orlowska (2004). This has special relevance for the visibility of model information for different users. The different processes are strongly interlinked with each other and can be seen as different views on the same process, where the various stakeholders have different access rights.

- A *Private Process* (PP) is hidden from other partners, e.g. because of intellectual property rights or in order to save business secrets (e.g. the supplier evaluation process details of a company which should be not public to external organisations).
- A *View Process* (VP) abstracts one or more PPs to a process interface that a company provides in collaboration with its partners. The combination of VP and PP enables companies to hide critical information from unauthorized partners. This has special relevance for the reusability of models. The FLUID-WIN B2(B2B) Business Process Model is a reference model which generally describes SCM- and service-provider-related business processes. Therefore, the model can be used to provide support during the implementation and introduction phase of FLUID-WIN services at the end user companies. These companies use the model as a template and adapt it to their own needs. Thereby, the companies can be sure that their internal process structure remains confidential.
- The *CBP* defines the interactions among two or more business entities, regardless if these entities are e.g. two manufacturers, a logistic provider and a manufacturer, or a logistic service provider and a financial service provider. An interaction is defined as a valid sequence of messages and/or other /material input/output exchanges.

The CBP model was very helpful to structure the modelling needs and levels for the FLUID-WIN B2(B2B) model. It served all needs occurring in this context, but did not provide all required guidance in the establishment of the new FLUID-WIN Model. However, it might be questionable if such guidance is possible at all when setting up novel kinds of models, or if in the contrary standardisation in this field might constrain creativity and innovation. Thus, no specific standardisation needs have been identified on this (more organisational) level. The technical point of view will be discussed later in this report.

Furthermore, in the framework of the SPIDER-WIN project (www.spider-win.de) an approach for the analysis of supply chain networks has been developed, which was based on reference models and a guideline with several components (Rabe and Weinaug 2005). This approach has been successfully applied for the analysis of requirements and potentials in regional supply networks, making the business processes of networks from Italy, Spain and Poland comparable and determining the consequences for new business processes and their software support (Rabe and Mussini 2005). Within the InterOp SDDEM approach, this method was generalized also taking into account similar approaches (Interop project 2007). The knowledge from this work could be very effectively used for the FLUID-WIN project. However, this work can not be considered any kind of standard, and thus is not discussed any further in this document.

4.1.3 SCOR and VCOR

There are few commonly accepted approaches for models in the manufacturing supply network area. The *Supply Chain Operations Reference* (SCOR) model was designed for the effective communication among supply chain partners (SCC 2006). SCOR is a reference model, as it incorporates elements like standard descriptions of processes, standard metrics and best-in-class practices. However, still SCOR has no real broad and common acceptance in industries, and the authors have experienced in their studies that most of the companies under consideration – especially the smaller ones – did not have any skills with respect to SCOR.

The *Value Chain Operations Reference* (VCOR) model (VCG 2006) follows a broader and more integrative approach than SCOR and supports the seamless and efficient management of distributed research, development, sales, marketing, sourcing, manufacturing, distribution and other processes. Provided by the Value Chain Group (VCC) the VCOR version 1.0 was a support tool to integrate process flow interdependencies across the product lifecycle, supply network and customer relationship domains, backed by a common language and standard metrics. The version 2.0 defines additional process flow interdependencies across tactical and operational level processes. For instance, the new finance and information process covers categories such as plan finance, plan information, govern finance, and govern information. Summarizing, VCOR has a more substantial approach than SCOR. However, VCOR has not even reached the industrial awareness of SCOR.

Finally, SCOR terminology and structures proposed by SCOR have been used as a starting point for the models developed within FLUID-WIN, but mainly for the analysis phase. For the B2(B2B) model, requirements have been to specific to be effectively dealt with by the (necessary generic) SCOR provisions. It might be questionable, if a more detailed SCOR standard would have been helpful.

4.2 Technological standards, Data Exchange

After a more broad analysis (reported within non-published deliverables), the two standards xCBL and UBL have been evaluated in detail for the implementation.

4.2.1 xCBL

The XML Common Business Library (xCBL) is a set of XML building blocks and a document framework that allows the creation of robust and reusable XML documents to facilitate global trading. It essentially serves a language that all participants in e-commerce can understand. This interoperability allows businesses everywhere to easily exchange documents for e-commerce, giving global access to buyers, suppliers, and providers of business services.

xCBL 4.0, the latest version considered, provides a smooth migration path from EDI-based commerce because of its origins in EDI semantics. xCBL will be able to support all essential documents and transactions for global e-commerce including multi-company supply chain automation, direct and indirect procurement,

planning, auctions, and invoicing and payment in an international multi-currency environment. xCBL 4.0 is the first version that uses XSDL as the canonical form. Previous versions all used SOX.

xCBL is the result of extensive collaboration between Commerce One® and the leading XML standards bodies, e-commerce enterprises, and hardware and software vendors, as well as analysis of existing e-commerce standards including Electronic Data Interchange (EDI) and RosettaNet, Industry leaders Compaq, Microsoft, SAPMarkets, and Sun Microsystems are leveraging xCBL 3.0 and xCBL 3.5 as a key standard in the development and delivery of business-to-business solutions.

xCBL began its life at Veo Systems in 1997. At that time it was called simply CBL, and was a research project partly funded by the Department of Commerce's Advanced Technology Program. CBL was developed to test the limits of XML for e-commerce and to identify requirements for XML design, development, and transaction tools and platforms. Subsequently, Veo invented the first object-oriented XML schema language; SOX, the Schema for Object-Oriented XML; as a result of the lessons learned in the first version of CBL.

In January of 1999, Commerce One acquired Veo Systems and the CBL technology. Commerce One saw the vision of conducting business electronically using XML that it embodied would help complete its transformation from an e-procurement company to a business internet company, and indeed, would transform the concept of e-commerce. The Veo CBL was tailored to support the Commerce One products and customers, which entailed making it interoperable with EDI (Electronic Data Interchange). This led to the creation of xCBL 2.0, and at that time the "x" was added to reflect the relationship with XML. xCBL 2.0 added a strong non-proprietary and interoperable semantic foundation for CBL, and gave companies using EDI a way to transform those applications to XML.

xCBL 3.0, released in December of 2000, represented a major broadening of scope and is more powerful than xCBL 2.0. It is rich enough to encode any e-commerce standard, and allows users to build customized documents from standard components. xCBL 3.0 saves developers and integrators enormous amounts of time and effort, and ensures that recipients are able to understand all documents that they receive when doing e-commerce. With version 3.5 of xCBL, support for the W3C Schema (full recommendation) is provided. This means that you could now choose between Commerce One's SOX, the W3C XSDL, Microsoft's XDR as well as the original DTDs when developing solutions that use xCBL. With the latest release, xCBL 4.0, XSDL is used as the schema canonical form and some initial alignment with standards defined by UBL.

4.2.2 UBL

Since its approval as a W3C recommendation in 1998, XML has been adopted in a number of industries as a framework for the definition of the messages exchanged in electronic commerce. The widespread use of XML has led to the development of multiple industry-specific XML versions of such basic documents as purchase orders, shipping notices, and invoices.

While industry-specific data formats have the advantage of maximal optimization for their business context, the existence of different formats to accomplish the same purpose in different business domains is attended by a number of significant disadvantages as well.

- Developing and maintaining multiple versions of common business documents like purchase orders and invoices is a major duplication of effort.
- Creating and maintaining multiple adapters to enable trading relationships across domain boundaries is an even greater effort.
- The existence of multiple XML formats makes it much harder to integrate XML business messages with back-office systems.
- The need to support an arbitrary number of XML formats makes tools more expensive and trained workers harder to find.

The OASIS Universal Business Language (UBL) is intended to solve these problems by defining a generic XML interchange format for business documents that can be extended to meet the requirements of particular industries. Specifically, UBL provides the following:

- A library of XML schemas for reusable data components such as “Address,” “Item,” and “Payment” — the common data elements of everyday business documents.
- A set of XML schemas for common business documents such as “Order,” “Despatch Advice,” and “Invoice” that are constructed from the UBL library components and can be used in generic procurement and transportation contexts.

A standard basis for XML business schemas provides the following advantages:

- Lower cost of integration, both among and within enterprises, through the reuse of common data structures.
- Lower cost of commercial software, because software written to process a given XML tag set is much easier to develop than software that can handle an unlimited number of tag sets.
- An easier learning curve, because users need master just a single library.
- Lower cost of entry and therefore quicker adoption by small and medium-size enterprises (SMEs).
- Standardized training, resulting in many skilled workers.
- A universally available pool of system integrators.
- Standardized, inexpensive data input and output tools.
- A standard target for inexpensive off-the-shelf business software.

UBL is designed to provide a universally understood and recognized commercial syntax for legally binding business documents and to operate within a standard business framework such as ISO 15000 (ebXML) to provide a complete, standards-based infrastructure that can extend the benefits of existing EDI systems to businesses of all sizes. UBL is freely available to everyone without legal encumbrance or licensing fees.

UBL schemas are modular, reusable, and extensible in XML-aware ways. As the first standard implementation of ebXML Core Components Technical Specification 2.01, the UBL Library is based on a conceptual model of information components known as Business Information Entities (BIEs). These components are assembled into specific document models such as Order and Invoice. These document assembly models are then transformed in accordance with UBL Naming and Design Rules into W3C XSD schema syntax. This approach facilitates the creation of UBL-based document types beyond those specified in this release.

4.3 Security and Trust

The general requirements for trust and security of web platform are:

- Standards for the identification (Strong Authentication)
- Standards for the authorization
- Standards for the verification
- Standards for privacy

4.3.1 Standards for the Identification (Strong Authentication)

Several commercial enterprises are supporting identity and authentication standards and creating de facto standards by implementing identity and authentication solutions. Among the most notable commercial enterprises promoting online worldwide identity and authentication solutions are VeriSign, IndenTrus, Microsoft, Certisign, Entrust, C&W HKT SecureNet, RSA and Cybertrust.

Authentication standards are being developed to support the establishment and on-going confirmation of identity. For each service, agencies must determine the level of identity-related risk. This level corresponds to a level of confidence required to establish an individual's identity and to an authentication key that pro-

vides on-going verification of identity. Other standards define data formats for identity-related data and message formats for confirmation of identity.

4.3.2 Standards for the Authorization

One of the most challenging problems in managing large networks is the complexity of security administration. Role-based access control (also called role-based security), as formalized in 1992 by David Ferraiolo and Rick Kuhn (Ferraiolo 2003), has become the predominant model for advanced access control because it reduces the complexity and cost of security administration in large networked applications.

With respect to *standards for the verification*, it is important to create a transparent trust model for online transactions. The purpose is to ensure that users gain confidence by doing business with companies that are committed to providing secure transactions. The underlying philosophy is to create and sustain a competitive, innovative and quality-driven approach to business.

Transparency is important to establish an atmosphere of trust and confidence and disclosure of a company's business information is as essential to this process as secure encryption technology.

Standards for consideration and approval for secure web platform include:

- SSL
- PGP encryption capability
- Proof of Organization
- Tax-identification number (or the international equivalent)
- Vendor or supplier reference as an established entity
- Financial institution and proof of a valid bank account

4.3.3 Standards for Privacy

Standards for privacy include symmetric and asymmetric cryptography. The most general and secure approach is the use of standard authentication protocols (e.g. ISO/IEC 9798). They are already widely used in networks or with smart cards. In these standardised protocols, cryptographic primitives are used. For symmetric authentication methods (the keys for sender and receiver are equal) MACs (message authentication codes) or symmetric encryption algorithms (e.g. DES, AES) are used. For asymmetric methods, where each party has a private and a public key, asymmetric encryption algorithms (e.g. RSA, ECC) or signature schemes are employed.

The FLUID-WIN Platform is aimed for communication between the users. As for any information sharing tool, the most important issue is the security of this communication.

Communication between external actors and the centralized platform is conveyed by three gateways. Therefore, the framework has two types of interoperability interfaces with different characteristics: internal and external. Hence, a detailed explanation of interoperability between gateways and the platform is provided in terms of infrastructure, implementation and security guidelines.

4.3.4 Internal Interfaces

Internal interfaces involve static actors. In fact, they connect FLUID-WIN gateways and the centralized platform. These FLUID-WIN modules run on specific servers and are managed by the consortium’s IT partners (Across Limits, Régens, Joinet). This impacts also the security aspect and policy:

- Trusty aspects have a minor relevance
- Security policy signed with gateway providers

As far as the communication is concerned, it is realized by:

- A unique protocol: the selected protocol for internal interfaces is Web services: SOAP over HTTPS.
- A well-defined message data set: regardless of the content and format of messages exchanged between the FLUID-WIN Platform and the three gateways, that is proprietary or adhering a certain standard, the message data set will always be the same. Messages flowing between the platform and the gateways are agreed among the consortium's IT partners.
- Synchronous processes: the process based on Web service requests and responses is always synchronous. When a gateway requests a service from the FLW Platform, the platform immediately responds and vice-versa.

4.3.5 External Interfaces

Element Considered and Structure Chosen

In contrary to the internal interfaces, the external interfaces involve dynamic actors. Dynamic means that the actors, linked to the Interoperability Framework, are not predefined. The number of actors will increase during the course of time. Thus, the approach to security aspects and policy is quite different from internal interfaces:

- Trust aspects have a great relevance
- Security policy changes on the basis of actors, and the start-up integration procedure will require all due information to set authentication and authorization aspects. For instance, if the actor requires a file transfer, the access to the FTP server must the defined. In case of using tunnelling on SSH, public and private keys must be exchanged between the specific gateway and the actor.
- A Service Level Agreement (SLA) must be defined and signed by every single actor. This SLA describes the quality of service (QoS) expected in terms of service availability.

The communication can vary in terms of:

- Protocol: the preferred protocol is Web service over HTTPS. Nevertheless, external actors do not always support this modality (for more details see chapters 7 to 9 of D12). Depending on the gateway, protocols can also be FTP/FTPs or secure channel (VPN, SSH).
- Messages data-set: often an actor cannot adhere to a precise standard for data-exchange. Thus, despite the fact that each FLW-Gateway will provide at least a standardized way to integrate the actors belonging to its domain, some integration process might require a special project. Hence, we expect to have many different message data-sets in terms of content and format. The gateway's task is to ensure a translation mechanism for these data-flows.
- Process type: the process can be both synchronous and asynchronous depending on the protocol. For instance, FTP requires an asynchronous process of data elaboration.

General Security Guidelines define how to implement the security in the internal interfaces, i.e. the communication between the FLUID-WIN Platform and the gateways.

The security is implemented at two levels:

- Transportation-level security.
- Message-level security

Transportation-level security refers to securing the connection between a client application and a Web service with Secure Sockets Layer (SSL), used to exchange Web services. Two types of SSL connections can be implemented:

- One-way SSL where the server is required to present a certificate to the client application

- Two-way SSL where both the client applications and the server present certificates to each other.

The solution implemented is the two-way SSL due to the fact that both platform and gateways, as counterparts, can act as client and server depending on who sends the request for a service.

Message-level Security is related to the mechanism provided by Web services. Data in a SOAP message are digitally signed or encrypted. This level provides security token propagation, message integrity, and message confidentiality. Security aspects of Web services have to be independent from the technology used to implement clients and servers: this is one of the fundamental requirements defined by the consortium's IT partners. Security in the Web services' industry is of great importance and a deciding factor for many corporations when moving to a Web services (WS) software architecture.

Currently, there are six extensions that reside on top of WS-Security and SOAP. Two of these have been defined but have not been published yet.

The project has chosen to focus on the WS-Security, WS-Trust, WS-Policy and WS-Secure Conversation modules. These encompass most of the security areas within the scenario of messages exchanges between platform and gateways.

Some basic requirements must be considered in a collaborative scenario:

- Identity Management: Each entity must be able to identity itself to the party it wants to communicate with
- Policy Management: Each entity enforces policies with other entities. E.g. message format, who has access to what, what one needs to process.
- Secure Messaging: authentication, confidentiality, integrity, non-repudiation

Figure 2 shows the WS-Framework Overview. In particular, the investigated aspects are: WS-Security. A standard set of SOAP extensions that can be used when building secure Web services to implement integrity and confidentiality. WS-Security makes use of the XML-Signature and XML-Encryption specifications and defines how to include digital signatures, message digests, and encrypted data in a SOAP message.

  - The XML-Signature specification is a joint effort of W3C and IETF. It aims to provide data integrity and authentication (both message and signer authentication) features, wrapped inside XML format.
  - W3C's XML-Encryption specification addresses the issue of data confidentiality using encryption techniques. Encrypted data is wrapped inside XML tags defined by the XML Encryption specification.
  - Security Assertion Markup Language (SAML) from OASIS provides a means for partner applications to share user authentication and authorization information. This is essentially the single sign-on (SSO) feature being offered by all major vendors in their e-commerce products. In the absence of any standard protocol on sharing authentication information, vendors normally use cookies in HTTP communication to implement SSO. With the advent of SAML, this same data can be wrapped inside XML in a standard way, so that cookies are not needed and interoperable SSO can be achieved.
  - eXtensible Access Control Markup Language (XACML) presented by OASIS lets the user to express his/ her authorization and access policies in XML. XACML defines a vocabulary to specify subjects, rights, objects, and conditions – the essential bits of all authorization policies in today's e-commerce applications.

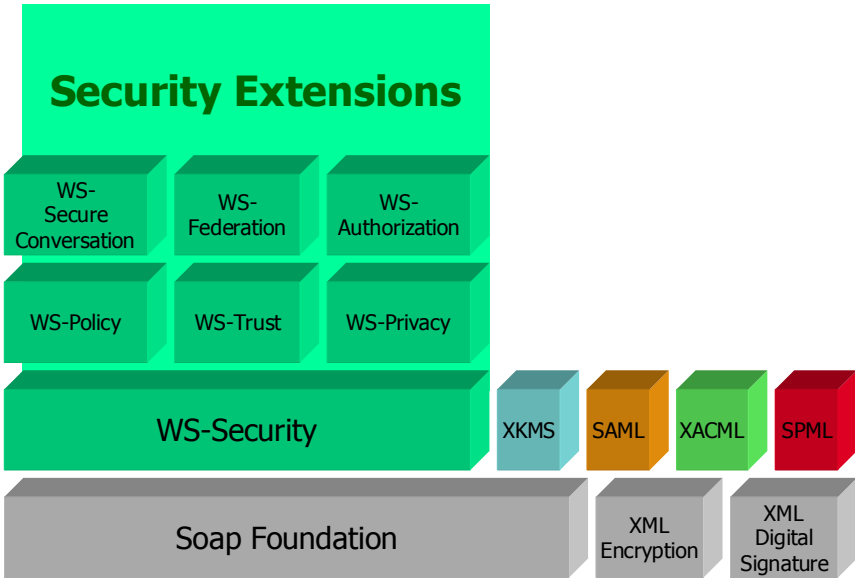

Fig. 2: WS-Framework overview

- WS-Trust. To provide a framework for requesting and issuing security tokens, and to broker trust relationships as sketched in the figures 3 and fig. 4. It enables the issuance and dissemination of credentials within different trust domains. If a message arrives without having the required proof of claims, the service should ignore or reject the message.
- WS-SecureConversation. WS-Security alone is not enough to address security issues; eavesdropper could sniff traffic of messages between parties cracking the symmetric key. WS-SecureConversation is used next to WS-Security. WS-SecureConversation defines mechanisms for establishing and sharing security contexts (lifetime conversation), and to provide secure communication across one or more messages, namely a security context and derived keys.
  - Establishing a security context is more beneficial for a series of messages between two parties because it is shared for the lifetime of the conversation.
  - Derived keys allow the involved parties to keep security updated during the interaction instead of relying on just one secret.

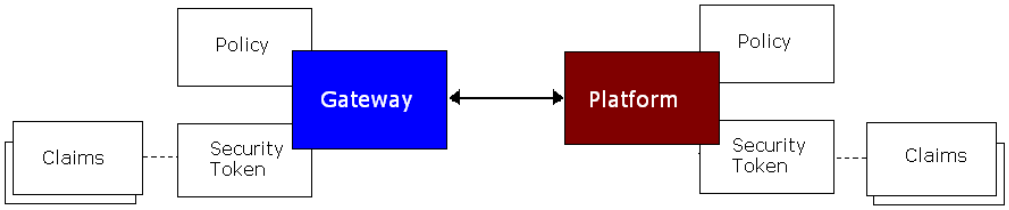

Fig. 3: WS-Trust elements representation

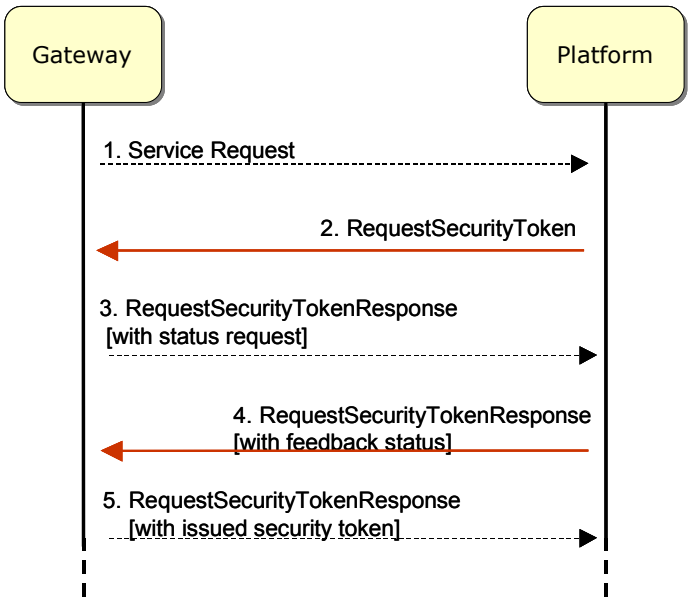

Fig. 4: Security Token Service

E-signature and Public Key Infrastructure (PKI)

X.509 (1988) is an ITU standard format for public key certificates. Public key certificates are a key element in the distribution and transfer of trust in public keys, which is itself is the basis for any other transfers of trust that depend upon public key cryptography.

The purpose of a public key certificate is to distribute public key information in a secure, well-managed fashion. Public key cryptography depends critically on the user of a public key having fell-founded confidence that the corresponding private key is known only to the person that they believe owns it. So, when checking a signature, the public key used must correspond to the intended signer's private key. Similarly, when encrypting data for a given recipient, the public key used must correspond to a private key that is known only to the intended recipient.

X.509 is based around the concept of a Certifying Authority (or CA) who checks the identity of some person or authorized entity who has also proved that they have possession of the private key. The CA then issues a Certificate, which is a data structure containing (among other things) the key holder's identity and a copy of their public key, all signed using the CA's private key. Then, if the recipient trusts the CA to properly identify the person, they can also trust that the identified person can also create signatures that check out using the public key signed by the CA.

An important property of a Public Key Certificate is that it can be made publicly available through untrusted channels without thereby compromising any trust that may be vested in the key.

Certificate Limitations and Revocation

The use of certificates is fine for checking that the intended signer did indeed have possession of the private signing key, but can never prove that nobody else also had access to the same key. This is an inherent problem with any PKI-based trust system. The relying party must trust that the signer's private key has not been compromised by disclosure to any other party.

A partial response to the problem of signing key disclosure to unauthorized parties is the Certificate Revocation List (CRL), which is a published list of certificates that have been revoked. Another partial response to this problem is that an X.509 certificate has a limited lifetime, after which it cannot be regarded as valid, and a new certificate must be obtained.

Yet another response to the problem is for the relying party to always check the certificate with the CA when using it to verify a signature. This may be expensive in terms of computation cost and communication delays, but is often regarded as the only acceptably safe option for high-value transactions.

Thus, one can see that trust in a public key depends on a number of factors, including trust in the key holder, both to live up to obligations conveyed by their signature, and also to properly guard their private key from disclosure to unauthorized parties, trust in the CA to properly verify the key holder's identity, and trust in the security of the technology used to create and verify signatures.

As described above, there is an implicit assumption that the user of a public key will trust the CA that was used to sign the corresponding certificate. This is not a practically scalable proposition.

So X.509 employs the idea of certificate chains, where each CA's public key is itself signed by a "higher" CA, and so on until a trusted "root" CA is encountered. Thus, a chain of certificates can link the holder of some key with a user of the corresponding public key to a common point of trust. Set against this, the longer the certificate chain the more scope there is for compromise of any one of the CA signing keys, which would effectively nullify the basis for trust in the end user keys thus protected.

The original X.509 design called for a single trusted root to the CA hierarchy. In practice, that has not been realized, but there are a number of certificate issuing organizations that are widely recognized (if not trusted), and whose public keys are widely distributed with web browsers and other software.

An unfortunate aspect of many kinds of computer interaction is that ordinary users don't have the real-world clues upon which to base their trust decisions ("would you buy a used car from this man?"). For the most part, non- technical computer users (and many technical ones too) have insufficient knowledge and understanding to make reasonable trust decisions, and end up relying on personal recommendations and credit card guarantees. The former is alright to a point, but is not fully applicable at Internet scale. The latter effectively puts credit card companies in the position of trusted certifying authorities for certain kinds of purchases, but doesn't extend so easily to other kinds of transaction (e.g. online medical advice).

Thus, public key certificates in general, and X.509 in particular, are technical approaches to a problem that cannot be solved wholly by technical means. X.509 certificates can carry additional information about policies and other non-technical aspects of trust decisions.

Syntax X.509 certificates are defined using ASN.1, per X.680 (1994), and encoded for transmission using Basic Encoding Rules (BER) per X.690 (1994)

Relationship to Trust Management

Public key certificates are a technical mechanism for conveying trust in (the authenticity of) public keys.

In relation to the message transfer framework described in section Interactions between autonomous communicating parties, public key certificates support the use of public key cryptography to provide authentication (by confirming the correct public key to verify a signature) and encryption (by confirming the correct public key to use in encrypting a message).

Related Specifications

- S/MIME (Ramsdell 1999) is designed to be used with X.509 certificates, and has explicit provision for carrying X.509 certificates as part of the signing and encryption key information.
- X.509 certificates can be used to certify public keys for use with OpenPGP (Callas et al. 1998) as an alternative or in addition to the PGP "web of trust", specific mechanisms for doing this are not widely deployed.
- X.509 certificates are quite complex, and their use involves the construction and analysius of ASN.1 BER-encoded data. This can be a significant barrier to implementation, and the XKMS (Ford et al. 2001) protocol is being developed to provide an easier way for XML applications to access the facilities provided by X.509 and other certificates.

4.4 Platform and Process Evaluation

Nowadays, IT engineers and managers are responsible for planning, designing, implementation and ranging software systems and IT environments based on end-users' needs. They are supported by various, already established standards for measuring or guidance of different aspects of software engineering. Partially, the standards focus on the software engineering process e.g. ISO 15504 "Information technology - Process assessment" (ISO 2004) and CMMI "Capability Maturity Model Integration" (CMMI Product Team 2002), partially they concentrate on the software product as outcome of the engineering, e.g. ISO 9126 "Software engineering - Product quality" (ISO/IEC 2001) and ISO 9241 "Ergonomics of human-system interaction" / (ISO/IEC 2006). Also the evaluation process itself is supported by ISO/IEC 14598 "Information technology - Software product evaluation" (ISO/IEC 1999-2001). Further approaches are the approaches from Ortegaet al. (2003), McCall et al. (1977), Boehm et al (1978), Grady and Caswell (1987) (FURPS) and Dromey (1996). In any case, the evaluation of systems and processes, before its implementation in practice, shall ensure that the end users get a safe and reliable system that matches their requirements.

With respect to the evaluation of a B2(B2B) platform, the most important norm is the ISO 9126 (ISO/IEC 2001). It defines product quality as a set of product characteristics. The characteristics that govern how the product works in its environment are called external quality characteristics, which include, for instance, Usability and Reliability. The internal quality characteristics is relating to how the product was developed; they include, for example, size, tests and failure rate, exchange rate, structure, etc. taken in the development of the product. Generally, ISO 9126 indicates that the software quality has been described in terms of one or several of the six characteristics listed below.

Each of these six characteristics is defined as a set of attributes that are supported by a relevant aspect of the software. The internal attributes of the software influence the external attributes; thus there are internal aspects and external aspects for the majority of the characteristics. In ISO 9126, the quality characteristics are defined with the associated sub-characteristics:

- Functionality: Suitability, Accuracy, Interoperability, Compliance, Security
- Reliability: Maturity, Fault Tolerance, Recoverability
- Usability: Understandability, Learnability, Operability
- Efficiency: Time behavior, Resource behavior.
- Maintainability: Analyzability, Changeability, Stability, Testability
- Portability: Adaptability, Installability, Conformance, Replaceability

The advantage of this model is that it identifies the internal characteristics and external quality characteristics of a software product. However, at the same time it has the disadvantage that some very important aspects like Process-Maturity, Flexibillity and Reusability are not overall covered (Ortega et al. 2003).

Based on a detailed survey and analysis of quality models, Ortega et al. (2003) have developed the "Systemic Quality model for Software Products" (fig. 5). It combines the advantages of several approaches and tries to close the gaps of the ISO 9126. Especially of interest for the B2(B2B) evaluation is the fact that the approach differentiate between product and process as well as efficiency and effectiveness.

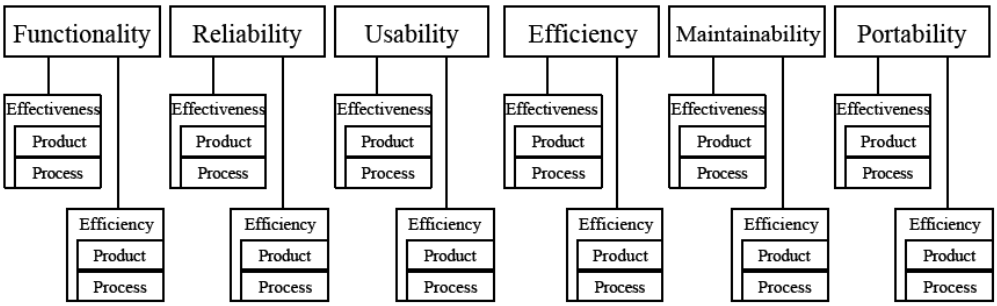

Fig. 5: of the Systemic Quality model for Software Products (Ortega et al. 2003)

5 Identified Requirements to Standards

5.1 Requirements to Business Process Modelling-Standards

As a consequence of the considerations above, no urgent needs for standards have been identifiable from the direct project activities. Obviously, new class structures have been necessary for modelling both in the analysis phase and the design phase. However, it seems questionable if a pre-defined standard would have simplified the work.

But, it should be recognized that the project work was made significantly more feasible by the common use of the IEM modelling method. The predefined reference models and guidelines as prepared in the field study phase of the project would not have been possible in this way, otherwise. This topic clearly addresses the interoperability with respect to business process models. There has been good process in the ATHENA project, leading to the POP* development, but this is still far from providing instant interoperability among companies that apply different modelling approaches.

SCOR was used and had to be extended. Also here it is not clear that a pre-defined extended standard could have fully served, but might have led to less amendments. This would not have massively contributed to saving time and work. Thus, there is no clear indication for the need to extend the SCOR definitions in view of FLUID-WIN experience.

5.2 Data Exchange Standards

In table 1 the comparison of FLW messages with fields mapped in UBL and xCBL standards is presented. This comparison shows areas of messages, which are strongly supported in existing standards (UBL, xCBL) as well as areas with less or without any mapping in mentioned standards. Both standards satisfy the FLUID-WIN requirements at similar level, with UBL doing slightly better (table 2).

	UBL			xCBL		
Messages	**Fields Mapped**	**Fields Not Mapped**	**Percentage of mapping**	**Fields Mapped**	**Fields Not Mapped**	**Percentage of mapping**
Purchase Order *Tot. Fields 15*	10	5	60%	12	3	80%
Active Forecast Information *Tot. Fields 5*	5	0	**100%**	4	1	95%
Logistic RFQ *Tot. Fields 30*	20	10	55%	19	11	60%
Logistic Quote *Tot. Fields 12*	11	1	90%	12	0	**100%**
Logistic Order *Tot. Fields 11*	8	3	75%	8	4	70%
Logistic Change Notification *Tot. Fields 7*	7	0	**100%**	6	1	90%

	UBL			xCBL		
Messages	**Fields Mapped**	**Fields Not Mapped**	**Percentage of mapping**	**Fields Mapped**	**Fields Not Mapped**	**Percentage of mapping**
Pro-Forma Invoice *Tot. Fields 22*	13	9	60%	13	9	60%
Acceptance/ Rejection of Pro-Forma Invoice *Tot. Fields 4*	2	2	50%	4	0	**100%**
Invoice *Tot. Fields 28*	16	12	55%	23	5	70%
Factoring Order *Tot. Fields 7*	6	1	90%	3	4	40%
Invoice Discounting Order *Tot. Fields 6*	5	1	90%	0	6	0%
Financial Quality Indicators *Tot. Fields 5*	0	5	0%	0	5	0%
KPI for ESP *Tot. Fields 4*	0	4	0%	0	4	0%
Logistic Quality Indicators *Tot. Fields 7*	0	7	0%	0	7	0%
Inventory Report *Tot. Fields 10*	0	10	0%	0	10	0%
Financial Status Information *Tot. Fields 3*	0	3	0%	0	3	0%
Status Information for Logistic Order *Tot. Fields 7*	0	7	0%	0	7	0%

Table 1: Comparison of UBL and xCBL covering with respect to FLUID-WIN message exchange

Percentage of mapping	Messages in UBL	Messages in xCBL
100%	2	2
80% - 99%	3	3
60 % - 79%	3	4
30% - 59%	3	1
0% - 29%	6	7

Table 2: Provision of required message content in percent

As seen from the comparison, the following areas are not mapped at all:

- Financial Quality Indicators – (FQ Indicators ID, FSP's ID, Formula Definition, Frequency, Result Format)
- KPI for ESP – (KPI Indicator ID, Formula Definition, Frequency, Result Format)
- Logistic Quality Indicators – (LSP, Customer, Period, Type, Subtype, Value, Unit)
- Inventory Report – (Sender (LSP), Good's Owner (LSP's Customer), Inventory Date, Inventory Line Items, Warehouse, Item Identification, Inventory Type, Separation, Serial Number, Quantity and Unit of Measurement)
- Financial Status Information – (FS – ID, Status Type, Default Value)
- Status Information for Logistic Order – (Status Information for Logistic Order, Logistic Order, Logistic Order's Reference Number, Logistic Task's Reference Number, Status Type, Date of Status Information, Comment, Accompanying Data)

Thus, the existing standards could be applied only with (proprietary, but published) extensions. Financial Quality Indicators, KPIs and Financial Status Information are absolutely necessary for FSPs, so as Logistics Quality Indicators, Inventory Report and Status Information for Logistic Order for LSPs.

Several areas could be mapped, partially:

- Purchase Order
- Logistic RFQ
- Logistic Order
- Pro-Forma Invoice
- Acceptance/ Rejection of Pro-Forma Invoice
- Invoice

Messages from these areas are mapped at 50% level at least by UBL.

Completely or almost completely mapped areas were:

- Active Forecast Information
- Logistic Quote – (message not mapped: Price and Currency)
- Logistic Change Notification
- Factoring Order - (message not mapped: Amount of Invoices Listed in Order)
- Invoice Discounting Order - (message not mapped: Company ID, FSP ID)

Analysing the differences between UBL and the FLUID-WIN requirements, it is obvious that messages have been well represented for the “classical” order exchange, while contributions to the integrated business including manufacturing, logistics, and finance is missing or at least incomplete. Taking into account that from one single project there will be no substantial generality, the demand of adding the identified missing information exchange to the UBL standard is not acceptable. However, the comparison table above can lead to substantial support of standardisation developments in the future, when the UBL standard will be extended in this direction, by delivering a well-proven list of messages and the corresponding message content.

5.3 Security and Trust Mechanism

Since there are standards which can be used for secure and trustable information sharing we are not going to ask for new requirements for standards. However, in this section we will indicate problems with application of the existing standards in practise.

The digital signature technology is commonly used in e-Business applications at the present. Usually there are two security standard levels:

- The first security standard uses elements of authentication and authorization, which are created of static password combinations, in some cases of static passwords and One-time Passwords (OTP).
- The second security standard realizes the authentication and authorization through the technology of digital signature (asymmetric cryptography). This type of electronic services has higher financial costs, but in comparison to the first one it is more reliable.

There exist various intermediates of security between the first and second security standard. It is especially OTP that is a more reliable form realized by the various features. These features randomly generate temporary static passwords (Token, TAN calculator, etc.). But, the mostly used type of security is a combination of security elements of the first and second security standard. It means that access to the secure zone is secured by a combination of static password and OTP (more detail is contained in the restricted deliverables D8 and D13, which could be made partially accessible to related standardisation bodies if required).

For secure access to the FLUID-WIN Platform as a commercial service it could be convenient to use a *digital signature*, which has been saved at the secure device (chip card, USB key) and protected by other safety elements (PIN and static password). It is necessary to take the existence of digital signature couple as granted, the first one for access purpose and cryptography and the second one for designation. The strength of this securing form is the fact that the method of digital signature is not breachable by “brute” force at the present time.

The weakness of this security method is insufficient knowledge of this method and infringement of all safety rules that are related to the physical security of digital signature storage site and safety elements, which allow for its operation. Therefore, it is necessary to work out the security policy, in which the method of usage, security principles and risks of improper use of this method will be exactly specified. Here a lot of work must be done, mainly by governmental support to use the digital signature in a critical mass of applications e.g. in eGoverment.

For example, it should be marked that FSPs have their own security policies. Especially larger financial institutions are hard to be convinced to adapt their policy as precondition to use the digital signature. In the fu-

ture, some banks might be enabling to use also digital signature in their services and becoming to be the registration authorities. It is likely that the FLUID-WIN Platform has to accept the policies of the certain FSPs, even if is this means that FLUID-WIN has to implement a set of different security mechanisms depending on the needs of each FSP.

Standardisation is, therefore, an important issue in this field. However, the outcome of the project is only the *need* for such standard, while FLUID-WIN can be quite easily adapted to the standard when it exists.

5.4 Platform and Process Evaluation

The evaluation scheme contains indicators which follow the ISO 9126 plus the differentiation by product and process indicators. However, many questions had to be set up, specifically, according to the functions, user roles, and user interfaces of FLUID-WIN. This additional information is project-specific and no reasonable standardisation is visible.

5.5 Conclusion

As the result of this investigation, there is no urgent need for further standardisation detected by the project, except in the security and trust domain. In the latter, only the need for such standard is emphasized, while the project has no specific demands on the details of such standard.

In the business process modelling domain as well as for the technological standards, the existing standards have been found not sufficient to cover the modelling elements required.

With respect to business process modelling (BPM), the IEM worked fine, but problems are clearly foreseen if interoperability would have been requested among the companies in terms of BPM. In “real life” the existence of models in other representations than IEM are very likely.

With respect to the message exchange, the best-fitting approaches xCBL and UBL lack information that inevitably has to be exchanged for the FLUID-WIN purposes. The list of gaps can be helpful as one important input to future extensions. However, the project experience will not deliver sufficient generality to claim for a specific extension of the standard.

6 References

Billings, Ch. W. (1989). Grace Hopper: Navy Admiral and Computer Pioneer, p. 74, Enslow. ISBN 089490194X

Boehm, B. W., Brown, J. R., Kaspar, H., Lipow M., McCleod, G. J., Merritt M. J. (1978) Characteristics of Software Quality. Amsterdam, North Holland

Callas, J., Donnerhacke, L., Finney, H., Thayer; R. (1998) OpenPGP Message Format , RFC 2440, November 1998

CMMI Product Team (2002) Capability Maturity Model Integration (CMMI). Carnegie Mellon University, Pittsburg

Dromey, G. (1996) Cornering the Chimera. IEEE Software, pp. 33-43.

Ferraiolo D.F., Kuhn D.R., Chandramouli R. (2003) Role-Based Access Control, Artech House, Norwood, Massachusetts, ISBN - 1580533701.

Ford, W.; Hallam-Baker, P.; Fox, B.; Dillaway, B.; LaMacchia, B.; Epstein, J.; Lapp, J. (2001) XML Key Management Specification (XKMS), W3C Note xkms, March 2001

Grady, R.; Caswell, D. (1987) Software Metrics: Establishing a Company-Wide Program. Prentice Hall.

Greiner, U.; Jäkel, F.-W. (2007) Process interoperability – From the idea to execution. In: T. Schulze, B. Preim, H. Schumann (eds.), Simulation und Visualisierung 2007, Magdeburg 8.-9. März 2007. San Diego, Erlangen: SCS Publishing House, pp. 141-153

Interop project: TG1 – SDDEM deliverables DTG1.2 und DTG1.3, 2007. http://interop-vlab.eu/ei_public_deliverables/interop-noe-deliverables/tg1-synchronisation-of-models-for-interoperability-sddem/

ISO/IEC (1999-2001) ISO/IEC 14598 Information technology –Software product evaluation, Part 1 to 6. ISO copyright office, Geneva

ISO/IEC (2001) ISO/IEC 9126 Software engineering - Product quality, Part 1 to 4. ISO copyright office, Geneva

ISO/IEC (2004) ISO 15504 Information technology - Process assessment, Part 1 to 4. ISO copyright office, Geneva

ISO/IEC (2006) ISO 9241-110 Ergonomics of human-system interaction, Part 110: Dialogue principles. ISO copyright office, Geneva

McCall, J. A., Richards, P. K., Walters G. F. (1977) Factors in Software Quality, Vols I, II, III, AD/A-049-014/ 015/055. Springfield, VA: National Technical Information Service

Mertins, K.; Jochem, R. (1999) Quality-oriented design of business processes. Kluwer Academic Publishers, Boston

Mylopoulos, J.; Papazoglou, M. (eds.): At your service: An overview of results of projects in the field of service engineering of the IST program. MIT Press Series on Information Systems, 2009 (to be published).

Ortega, M.; Pérez, M.; Rojas, T. (2003) Construction of a Systemic Quality Model for evaluating a Software Product. In: Software Quality Journal, 11:3, July 2003. Kluwer Academic Publishers, pp. 219-242.

Rabe, M.; Mussini, B. (2005) Analysis and comparison of supply chain business processes in European SMEs. In: European Commission (ed.): Strengthening competitiveness through production networks – A perspective from European ICT research projects in the field 'Enterprise Networking'. Luxembourg: Office for Official Publications of the European Communities, pp. 14-25

Rabe, M.; Weinaug, H. (2005) Methods for Analysis and Comparison of Supply Chain Processes in European SMEs. 11th Conference on Concurrent Engineering (ICE), Munich, pp. 69-76

Ramsdell, B. (1999) S/MIME Version 3 Message Specification, RFC 2633, June 1999

SCC (2006) Supply-Chain Operations Reference Model. Supply-Chain Council, http://www.supply-chain.org, visited 10.11.2006

Schulz, K., Orlowska, M. (2004) Facilitating cross-organisational workflows with a workflow view approach. Data & Knowledge Engineering 51(1), pp. 109-147

VCG (2007) Value Reference Model. Value Chain Group. http://www.value-chain.org/, visited 08.11.2007

X.509 (1988) International International Telephone and Telegraph Consultative Committee, "Information Technology - Open Systems Interconnection - The Directory: Authentication Framework", CCITT Recommendation X.509, November 1988.

X.680 (1994) International International Telephone and Telegraph Consultative Committee, "Specification of Abstract Syntax Notation One (ASN.1): Specification of Basic Notation", CCITT Recommendation X.680, July 1994.

X.690 (1994) International International Telephone and Telegraph Consultative Committee, "ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", CCITT Recommendation X.690, July 1994.

Interop project: TG1 – SDDEM deliverables DTG1.2 und DTG1.3, 2007. http://interop-vlab.eu/ei_public_deliverables/interop-noe-deliverables/tg1-synchronisation-of-models-for-interoperability-sddem/