INFORMATION SHARING PLATFORMS AND RELATED STANDARDS

Jozef BUCKO, Peter MIHÓK, Martin VEJAČKA
Department of Applied Mathematics and Economic Informatics, Faculty of Economics,
Technical University of Košice, Nemcovej 32, 042 00 Košice, Slovak Republic, tel.: +421 55 602 3269, e-mail: jozef.bucko@tuke.sk

ABSTRACT

Different electronic services offered in e-banking, e-commerce, e-government, e-manufacturing, e-learning, etc. are becoming to be a part of everyday life for people everywhere. A communication portal has become universal solution in all cases from common communication between persons or information and data interchange up to e-business. For the creation of quality portal for information interchange of sensitive character, it is necessary to know standards dedicated to this purpose. The main requirement for these platforms is document and data interchange, what presumes usage of well-known and attested standards. Using the portal also imposes trust of users. One way of building the trust in a platform is usage of accepted standards. In this paper we concentrate on two groups of standards – standards for technological data and information exchange and standards for interchange security.

Keywords: *standards, security, trust, digital signature*

1. INTRODUCTION

The scope of this paper is to present standardisation and pre-normative activities within the framework of FLUID-WIN project (more details on: www.fluid-win.de), where we identified the areas and domains of the standardisation activities and 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 eventual motivations for new standards? What standards in what research areas are lacking? Do we need some enhancement of the existing standards and are there any other information useful to contribute to standardisation activities?

The FLUID-WIN Project covers the material flow among the European supply network as well as the financial flow associated with this supply. The FLUID-WIN will develop models that allow customisation of the work-flow [1].

The new process model includes [1]:

- 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 software releases).
- Interfaces, which are specified publicly and supported by guidelines and examples. Here, interfaces are shown as logical interfaces, i.e. they model the necessity of data exchange.
- 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.

FLUID-WIN set priorities on pre-normative work. The new B2(B2B) Model is published and available as input for the amendment of running standards to the specific requirements of networks, especially of smaller enterprises. Moreover, the project uses SCOR as the base for the definition of classes and processes with respect to the production supply, and carefully document amendments done in the project as a potential input to the further development of SCOR [2]. Other standards, which the FLUID-WIN project adheres and disseminates, include the XML catalogue standards like xCBL and cXML. Furthermore, FLUID-WIN respects major EDI standards, which enable companies to communicate with each other, regardless of their internal systems. This includes but is not limited to ANSI, ASC X12, AS2, EDIFACT and XML.

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 standardizing organizations indicates that a document purporting to be a "standard" does not necessarily have the support of many parties. As Grace Hopper said "The wonderful thing about standards is that there are so many of them to choose from" [3]. 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) [4],[5], [6],[7]
- 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)

In this paper we give an overview of standards, which have been selected and implemented in data exchange and trust and security areas.

2. TECHNOLOGICAL AND DATA EXCHANGE STANDARDS

Two standards: xCBL and UBL were considered during the project in detail.

- *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 as 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. [8]

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 multicompany supply chain automation, direct and indirect procurement, planning, auctions, and invoicing and payment in an international multicurrency environment. [8]

- *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.

The OASIS Universal Business Language (UBL) is defining a generic XML interchange format for business documents that can be extended to meet the requirements of particular industries [8]. Specifically, UBL provides a library of XML schemas for reusable data components such as "Address", "Item" and "Payment" and 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. [9]

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. [10], [11]

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. [12], [13], [14]

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) [12]. 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. 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 easier 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. [13], [14]

In FLUID-WIN project the comparison of FLW messages with fields mapped (necessary for FLUID-WIN platform function) in UBL and xCBL standards was performed. This comparison showed 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 data interchange standards satisfied the FLUID-WIN requirements at similar level, with UBL doing slightly better (table 1). [14]

Table 1 Provision of required FLUID-WIN platform message content in percent

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

This table shows that many messages necessary for the FLUID-WIN platform functions were not covered satisfactory by both surveyed XML-based standards. The areas with no coverage in considered standards mainly matched with innovative functions of the FLUID-WIN platform (e.g. generation of financial status information, logistic order information, warehousing information and key performance indicators generation). Also messages covering financial and logistics documents interchange were not covered seamlessly. This problem can be solved by amending of necessary messages to the best fitting UBL standard to satisfy needs of the FLUID-WIN platform functionalities in future. This modified standard might be used at the platform’s specific conditions and requirements, but its exploitability outside of the FLUID-WIN environment is an on-coming question.

3. SECURITY AND TRUST STANDARDS

The general requirements for trust and security of web platform are [13], [15], [16]:

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

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

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 [17], 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 [16]:

- 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

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 web platform is aimed for communication between the users. As for any information sharing tool, the most important issue is the security of this communication [17].

3.4. Standards for verifications

X.509 (1988) is an ITU standard format for public key certificates [18]. Public key certificates are a key element in the distribution and transfer of trust in public keys, which 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) which checks the identity of some person or authorized entity that has also proved that they have possession of the private key. 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. Public key certificates are a technical mechanism for conveying trust in (the authenticity of) public keys [19].

In relation to the message transfer 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).

3.5. Security and trust mechanism

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

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.

For secure access to the web platform as a commercial service it could be convenient to use a digital signature. 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 breakable by "brute" force at the present time.

4. CONCLUSIONS

In the business process-modelling domain as well as for the technological standards, the existing standards are still not sufficient to cover all modelling elements, which are required. With respect to the message exchange, the best fitting approaches xCBL and UBL lack information that inevitably has to be exchanged for the information exchange purposes. The list of gaps can be helpful as one important input to future extensions. However, our experience will not deliver sufficient generality to claim for a specific extension of the standard. The best solution to cover the FLUID-WIN platform's needs was to extend the current standard (UBL in data exchange area) for its specific conditions. Standards for security and trust and digital signature technology are used more commonly and they cover needs of this platform satisfactory therefore there is no need to modify them at the FLUID-WIN environment and they will be used without any change.

ACKNOWLEDGMENTS

This work has been partly funded by the European Commission through IST Project FLUID-WIN: Finance, logistics and production integration domain by web-based interaction network (No. IST-FP6-27083). We wish to acknowledge our gratitude and appreciation to all the FLUID-WIN project partners for their contribution during the development of research presented in this paper.

REFERENCES

[1] REVÉSZOVÁ, L. – BUCKO, J. – MIHÓK, P.: *Modelling of e-services*. In: Ambient Intelligence Perspectives: Ambient Intelligence and Smart Environments: Selected papers from the First International Ambient Intelligence Forum 2008, ISSN 1875-4163, vol. 1 (2009), pp. 203-210.

[2] BOLSTORFF, P. – ROSENBAUM, R.: *Supply Chain Excellence*. New York: AMACOM, 2007. ISBN 0-8144-0926-1, pp. 7-15.

[3] BILLINGS, Ch. W.: *Grace Hopper: Navy Admiral and Computer Pioneer*. Enslow. 1989, ISBN 089490194X, pp. 74.

[4] ISO/IEC 14598 Information technology –Software product evaluation, Part 1 to 6.

[5] ISO/IEC 9126 Software engineering - Product quality, Part 1 to 4.

[6] ISO/IEC 15504 Information technology - Process assessment, Part 1 to 4.

[7] ISO/IEC 9241-110 Ergonomics of human-system interaction, Part 110: Dialogue principles.

[8] XML.org: UBL standardization – The OASIS Technical Committee, 2008. http://ubl.xml.org/wiki/about-the-oasis-ubl-technical-committee

[9] FORD, W. – HALLAM-BAKER, P. – FOX, B. – DILLAWAY, B. – LAMACCHIA, B. – EPSTEIN, J. – LAPP, J.: *XML Key Management Specification (XKMS)*, W3C Note XKMS, March 2001.

[10] XML Common Business Library: XML Common Business Library (xCBL), version 4.0 Specifications, 2003. http://www.xcbl.org/xcbl40/documentation.shtml

[11] XML Common Business Library: XML Common Business Library (xCBL), earlier versions, 2002. http://www.xcbl.org/earlierversions.shtml.

[12] XML.org: UBL 2.0 Standard – UBL Specifications, 2006. http://ubl.xml.org/wiki/ubl-specifications

[13] GULIANO, A. – AZZOPARDI, J. – MIHÓK, P. – BUCKO, J. – RAMKE, Ch.: *Integration of Financial Services into Multidisciplinary Web Platforms.* In: New Technologies for the Intelligent Desing and Operation of Manufacturing Networks: Results and Perspectives from the European AITPL Project Cluster. Stuttgart: Fraunhofer IRB Verlag, 2007, ISBN 978-3-8167-7520-1, pp. 149-162.

[14] WEINAUG, H. et al.: FLUID-WIN. Deliverable D24. Requirements to Standards. Berlin: Fraunhofer IPK, 2009. http:// www.fluid-win.de

[15] MIHÓK, P. – BUCKO, J. – DELINA, R. – PAĽOVÁ, D.: *Trust and Security in Collaborative Environments.* In: Enterprise Interoperability 3: New challenges and industrial approaches. London: Springer Verlag, 2008, ISBN 978-1-84800-220-3, pp. 135-143.

[16] PCI Security Standard: PCI Security Standards Policy. 2007. https://www.pcisecuritystandards.org/tech/index.htm

[17] FERRAIOLO, D. F. – KUHN, D. R. – CHANDRAMOULI, R.: (2003) Role-Based Access Control, Artech House, Norwood, Massachusetts, ISBN - 1580533701.

[18] TRUSTe: Security guidelines 2.0., 2005. http://www.truste.org/pdf/ SecurityGuidelines.pdf

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

Received March 1, 2010, accepted September 9, 2010

BIOGRAPHIES

Jozef Bucko was born on 1.4.1972. In 1995 he graduated (MSc) in the field of Mathematics and Physics at the Faculty of Science at Pavol Jozef Šafárik University in Košice He defended his PhD in the field of Discrete Mathematics in 2000; his thesis title was "Uniquely partitionable graphs". Since 1998 he is working as a tutor with the Department of Applied Mathematics and Business Informatics. His scientific research is focusing on security and trust of web platforms and e-services. In addition, he also investigates questions related with modelling business e-processes.

Peter Mihók was born on 2.4.1949. In 1972 he graduated (MSc) in the field of Mathematics at the Faculty of Science at Pavol Jozef Šafárik University in Košice He defended his PhD in the Geometry and Topology in 1983 with thesis on graph invariants. Since 2000 he is working as a Head of the Department of Applied Mathematics and Business Informatics. His research interest is in the area of discrete mathematics – graph theory: object systems and the structure of their properties. He is also interested in information systems, user requirements engineering, modelling languages and tools.

Martin Vejačka was born on 7.7.1982. In 2006 he graduated (MSc) in the field of Finance, Banking and Investment at the Faculty of Economics at Technical University in Košice. Since 2007 he is PhD. student in the field of Finance at the Faculty of Economics at Technical University in Košice. His PhD. thesis title is "Integration of financial services on web platforms". It is to be defended at September 2010. His scientific research is focusing on electronic financial services and their web integration.