Chapter 19
A Secure and Trustful e-Ordering Architecture (TOES) for Small and Medium Size Enterprises (SMEs)

Spyridon Papastergiou
University of Pireaus, Greece

Despina Polemi
University of Pireaus, Greece

ABSTRACT

Although various European Union (EU) directives have established the proper legal framework for the provision of a trustful, legally accepted cross border transaction via electronic means, the consumers are still hesitant to use e-commerce. Lack of confidence with regard to the protection of privacy and security of electronic transactions is among the main reasons. This chapter attempts to form the appropriate confidence framework describing a set of privacy and security requirements that must be taken into account for e-ordering systems. In addition, it presents a trustful e-ordering architecture (TOES) that achieves to address these requirements based on extensible markup language (XML), XML cryptography, public key infrastructure (PKI), Web services policy language (WSPL), and Web services. TOES is an open, secure, interoperable, and affordable e-ordering system that respects the EU legislation.

INTRODUCTION

A significant effort was made during the last decade for the development of the proper infrastructure that would provide most of the appropriate elements that are essential for the international adoption of electronic commerce (e-commerce). The most important requirements that were addressed are the international interconnection that was achieved by the rapid development and spreading of Internet, the domination of extensible markup language (XML) and XML schemas that guaranteed the interoperability among different architectures, different platforms, and different development languages, and finally the development of standards such as the XML common

business library (xCBL) that provide a set of XML building blocks and a document framework that allows the creation of robust, reusable XML documents in order to facilitate the global trading.

Nevertheless, a crucial role on the adoption of e-commerce plays the definition of the European Union legal framework. The current legal framework achieves to cover the legal substance of technological possibilities of electronic commerce only at one point. The directive on electronic commerce (2000/31/EC) (European Parliament, 2000) has established a legal framework for suppliers, making it possible for them to do business with customers in other member states without having to apply the laws of those member states.

At the same time, there is a set of European Union directives that clarify the principles that are applied in some of the e-commerce's processes. The Council Directive 2001/115/EC (European Parliament, 2001) of December 20, 2001, amends Directive 77/388/EC with a view to simplifying, modernizing, and harmonizing the conditions laid down for invoicing in respect of value added tax and the Directive 2004/18/EC (European Parliament, 2004) of March 31, 2004, on the coordination of procedures for the award of public works contracts, public supply contracts, and public service contracts constitute representative examples. The chapter is focused on a specific aspect of e-commerce, the electronic ordering (e-ordering) service. The legal framework that concerns the e-ordering service is determined mainly by the EU Directive 2000/31/EC.

The ordering service as a process of e-commerce should allow for true business-to-business (B2B) secure collaboration by giving the possibility to salesmen and purchasers to execute trustful processes of electronic trading for opening new markets. Among the advantages that e-ordering offers include are the generation of more revenue, improvement of sales efficiency, increase of customer retention, accuracy and efficiency of sales, and elimination of costs.

The e-ordering implementations have to satisfy several security and privacy requirements. These requirements arise from the fact that the ordered documents may contain business data (e.g., VAT code, items) or private data that should not be revealed or modified. They should be trustful documents requiring all four dimensions of security (i.e., confidentiality, integrity, authenticity, nonrepudiation) and privacy.

The existing e-ordering systems discriminated in two types. The first are ERP inclusive systems (e.g., SAP) that manage the sources within and beyond an enterprise. These systems are not affordable for small and medium enterprises (SMEs), blocking them from entering B2B profitable applications. In addition, although they satisfy several security requirements, they do not achieve interoperability. The second type is customized solutions offering e-ordering as an autonomous service. Existing systems of this type ignore various security and privacy requirements.

The purpose of this chapter is the presentation of the security and privacy requirements of an e-ordering service, as well as the proposition of an open, affordable, and scalable e-ordering architecture that satisfy these requirements complied with EU regulations and directives. The proposed system, in order to meet these objectives, is built using open technologies, such as XML, XML cryptography, public key infrastructure (PKI), Web services policy language (WSPL), and Web services.

The rest of this chapter is organized as follows. Section 2 provides an overview of the legal framework which supports electronic ordering, it illustrates the fundamental security and privacy requirements of e-ordering and presents the existed e-ordering implementations. Section 3 describes in detail the e-ordering system architecture and its components. Section 4 provides an assessment (technological, organizational, legal, and business) of trustful e-ordering architecture (TOES) architecture and finally Section 5 presents our conclusions and areas for further research.