Secure Business Transaction based on ebXML
Applying Web Service Security

Dongkyoo Shin* and Dongil Shin
Department of Computer Engineering, Sejong University
98, Gunja-Dong, Gwangjin-Gu, Seoul 143-747, Korea
{shindk, dshin}@sejong.ac.kr
*Corresponding Author

Abstract. ebXML business transaction models are proposed which allow trading partners to securely exchange business transactions by employing Web service security standard technologies.

Keywords: electronic commerce, ebXML, Web service security, secure business transaction

1 Introduction

ebXML (Electronic Business using eXtensible Markup Language) is a modular suite of specifications for the XML-based global infrastructure for e-business transactions, and provides a standard method to exchange business messages, conduct trading relationships, communicate data in common terms and define and register business processes [1, 2]. The technical infrastructure of ebXML is composed of the following major elements: Messaging Service, Registry, Trading Partner Information (It consists of two specifications: CPP (Collaboration Protocol Profile) and CPA (Collaboration Protocol Agreement)), Business Process Specification Schema, Core Components.

There are well-known conventional security technologies that can be used by ebXML implementers to resolve the risks [2]: user-id and password, PKI (Public Key Infrastructure), SSL (Secure Socket Layer), S/MIME (Secure Multi-Purpose Internet Mail Extensions). Web Service security technologies emerging recently have extensibility and flexibility suitable for ebXML security implementation such as encryption, digital signature, access control and authentication. XML digital signatures [3] and SAML (Security Assertion Markup Language) [4] can be exploited to solve the unauthorized transactions and fraud problems in electronic business systems. XML digital signatures are used in ebXML to provide data integrity on messages, existing authentication and authorization schemes as well as non-repudiation between entities. SAML is recommended to provide identification, authentication and authorization and often used with XACML (eXtensible Access Control Markup Language) [5] to allow or deny access to an XML resource. XML Encryption [6] is recommended to solve the loss of confidentiality problem. Also XKMS (XML Key Management Specification) [7] is recommended for key
management as a substitute for PKI.

2. Secure Business Transaction Models based on the ebXML

A high-level use case scenario for two trading partners is explained based on the ebXML technical architecture specification [1] as follows.

Fig. 1. The first model: Update of CPP (Collaboration Protocol Profile)

*Company A* will first review the contents of an ebXML Registry, especially the registered business processes that may be downloaded or viewed. Based on a review of the information available from an ebXML Registry, *Company A* can build or buy an ebXML implementation suitable for its anticipated ebXML transactions. The next step is for *Company A* to create and register a CPP with the registry. *Company A* might wish to contribute new business processes to the registry, or simply reference
available ones. The CPP will contain the information necessary for a potential partner to determine the business roles in which Company A is interested, and the type of protocols it is willing to engage in for these roles. Once Company A is registered, Company B can look at Company A’s CPP to determine that it is compatible with Company B’s CPP and requirements. At that point, Company B should be able to negotiate a CPA automatically with Company A, based on the conformance of the CPPs, plus agreement protocols, given as ebXML standards or recommendations. Finally, the two companies begin actual transactions.

Fig. 2. The second model: Exchange of Business Transactions

Based on the scenario, we propose two ebXML business transaction models ensuring the trust relationship within the real trading partners. The first model performs a user authentication and updates the CPP in the registries. The second model performs business transactions within the trading partners. These models will explain how each Web service security technology solves the risks for ebXML.

We showed how each Web service security technology meets the ebXML standard by constructing the experimentation software and validating messages between the trading partners.

References