A SECURE FRAMEWORK ON RFID-ENABLED SUPPLY CHAIN WITH WEB SERVICES

Dong-Her Shih, Po-Ling Sun, Department of Information Management, National Yunlin University of Science and Technology, 123, Section 3, University Road, Touliu, Yunlin, Taiwan.
Jinsheng Roan, National Chung Cheng University, 168, University Road, Min-Hsiung Chia Yi, Taiwan.

ABSTRACT

This paper outline security concerns around data being shared over the Internet through the EPCglobal Network and depict how Web Service Security framework can work to provide a simple, multi-business exchange of data across the Internet, and highlights in protecting sensitive data for EPCglobal Network.

INTRODUCTION

Radio Frequency Identification (RFID) has recently received a lot of attention as an augmentation technology in supply chain management (SCM) because RFID are thought to improve supply chain end-to-end visibility [1]. The operation of RFID-enabled supply chain model is shown in Figure 1. When information is all pointed to over a public network, security does become a concern. Because of security and privacy concerns, the EPC-IS will be fragmented across the supply chain, with each party handling the object being responsible for updating their own internal database with information about the tagged object while it is in their custody. The EPC-IS must be able to define precisely which subset of data each authenticated user or group of users is entitled to access, as shown in Figure 2. There are various aspects of security that need to be considered as below Table 1 [2, 3].

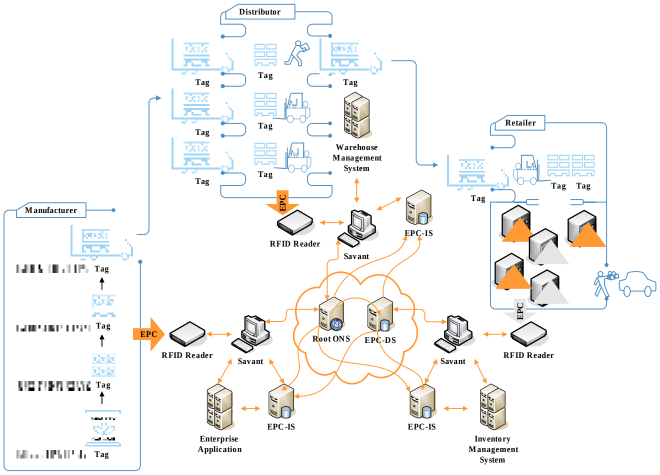


Figure 1 A Graphical Representation of EPC Global Supply Chain Model

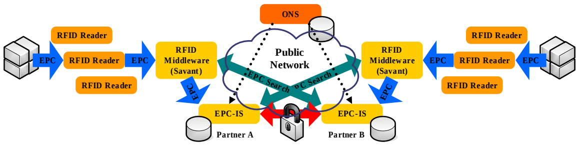
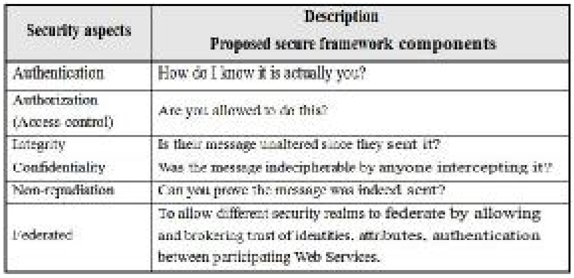


Figure 2 EPC-IS data security



Security aspects	Description Proposed secure framework components
Authentication	How do I know it is actually you?
Authorization (Access control)	Are you allowed to do this?
Integrity	Is their message unaltered since they sent it?
Confidentiality	Was the message indecipherable by anyone intercepting it?
Non-repudiation	Can you prove the message was indeed sent?
Federated	To allow different security realms to federate by allowing and brokering trust of identities, attributes, authentication between participating Web Services.

Table 1 data Security challenges and definition

PROPOSED FRAMEWORK

RFID achieve data shared and exchanged among industry wide EPCglobal Network through ONS; Web Services achieve data shared and exchanged among Web-based applications though UDDI [4, 5]. And what it more, Web Services Security model provides secure interoperability across platforms, organizational boundaries, and multi-language applications. To fully realize this functionality, the model needs to ensure security within Web Services environment. We present here a secure industry wide EPCglobal Network architecture with Web Service Security for the distributed RFID systems environment, as shown in Figure 3(a), and the secure binding process is shown in Figure 3(b).

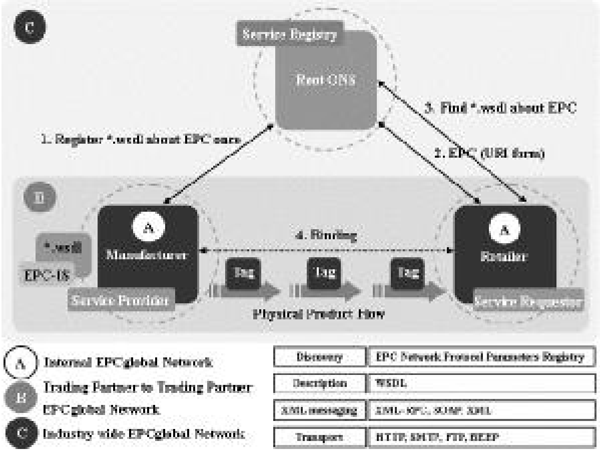


Figure 3(a) Integer industry wide Network with WS-Security

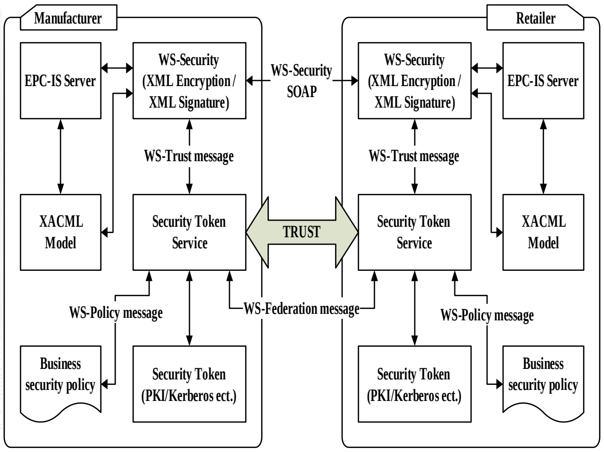


Figure 3(b) the secure binding process with WS-Security

Register Web Services in EPCglobal Network

A document specifying a service name must contain the following template. This template is then entered into the registry as soon as the document is published [6]: Service Name, Functional Specification, Valid URI schemes, Security Considerations.

Find Services in EPCglobal Network

The ONS provides a global lookup service to translate an EPC into one or more Internet Uniform Reference Locators (URLs) where further information on the object may be found. These URLs often identify an EPC-IS, though ONS may also be used to associate EPCs with web sites and other Internet resources relevant to an object.

Binding Secure EPCglobal Network with WS-Security

Increasingly, as inter-organizational integrations becomes commonplace, the need for federation of security attributes becomes more and more important. It is this desire to establish identity in one organization with one set of policies and procedures under a trust domain and be able to assert rights to do things in a separate and distinct trust domain. The above-mentioned Figure 20(b) describes the high-level architecture of our approach. The architecture consists of five main components: 1) XML

Signature [7, 8], 2) XML Encryption [7, 8], 3) WS-Security (WSS) [7, 9], 4) XACML model [10], and 5) Web Services Federation [11]. Figure 4 illustrate how the Web Service Security framework we proposed applies to secure RFID data for consumer goods supply chain.

We claimed that the following various aspects of security described in [2, 3] are achieved in our secure framework, as shown in Table 2.

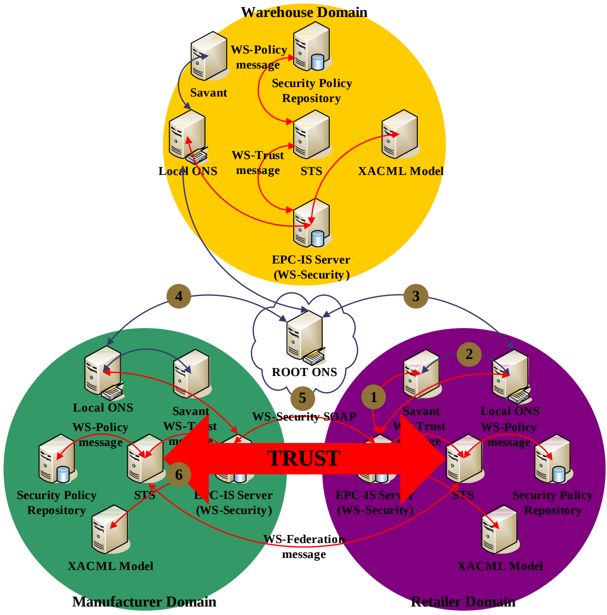
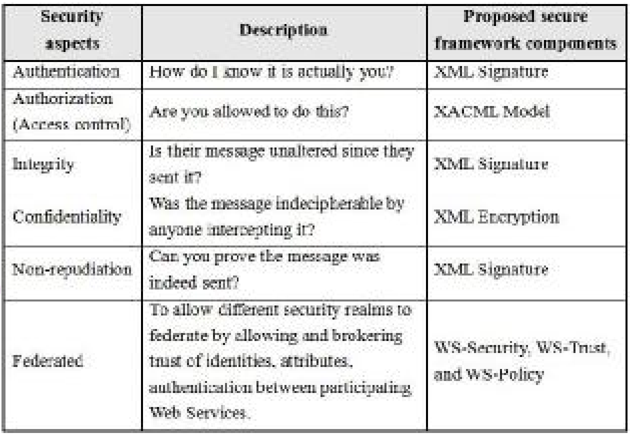


Figure 4 Secure RFID data for supply chain with WS-Security.



Security aspects	Description	Proposed secure framework components
Authentication	How do I know it is actually you?	XML Signature
Authorization (Access control)	Are you allowed to do this?	XACML Model
Integrity	Is their message unaltered since they sent it?	XML Signature
Confidentiality	Was the message indecipherable by anyone intercepting it?	XML Encryption
Non-repudiation	Can you prove the message was indeed sent?	XML Signature
Federated	To allow different security realms to federate by allowing and brokering trust of identities, attributes, authentication between participating Web Services.	WS-Security, WS-Trust, and WS-Policy

Table 2 aspects achieved in our secure framework

CONCLUSIONS

RFID and the EPCglobal Network have the potential to revolutionize business processes across a wide range of industries. RFID systems provide an automatic means to quickly, accurately, reliably, and flexibly capture information. Companies not only want to know where their assets are, they also want to selectively and securely share information with their trading partners to enable "anywhere awareness" business interactions. Here we proposed a Web Service Security framework to secure RFID data for Supply chain. Building on these initial secure concepts, we can continue to work with customers, partners and industry wide to provide follow-on more sophisticated scenarios for federated security which include secure conversations, federated trust, and authorization.

(References are upon request)

Acknowledgment: The authors would like to thank the National Science Council of Taiwan for providing support to this research through grant (NSC 94-2218-E-194-005) and (NSC 94-2213-E-224-036).