

# 以SAML為基礎之安全採購系統研究

盧振華、曹偉駿

E-mail: 9314337@mail.dyu.edu.tw

## 摘要

隨著網際網路的全球普及，企業間的電子交易日益頻繁，大量取代以往用電話及傳真的交易模式，因此企業間的交易模式逐漸從利用專線的EDI 轉變成為利用Internet 的XML 交易模式，費用得以大幅降低。然而，XML 本身並無法提供完整的網路交易安全的特性，例如：(1)身分驗證-Authentication (2)授權-Authorization (3)不可否認性-Non Repudiation，所以必須藉由SAML 安全機制來保護交易資料的安全。為了提供安全的Web Service，除了目前常用的SSL 安全機制外，尚有Microsoft Passport 及SAML 兩種。由於SSL 安全性已被RSA 公司證明安全性不足[23]，並不適合作為B2B 的安全機制。此外，Microsoft Passport 必須使用Microsoft 作業平台才能提供服務，對其他系統目前則無法支援，如UNIX，LINUX，PDA 或其他非Microsoft 的交易平台等，因此為了適合不同裝置及作業平台的通用性，本研究捨棄Microsoft Passport，採用SAML 標準作為研究基礎。SAML 為OASIS 提出之新一代電子商務交易安全標準，此標準具有：(1) Authentication Assertion (2) Attribute Assertion (3) Authorization Decision Assertion 的特性，這些方法可達到提高XML 架構的安全性。除此之外，本研究亦模擬一個採購系統，在Web-based 部分結合SAML 安全機制，來滿足B2B 網路交易安全的特性。

關鍵詞：SAML，XKMS，B2B，XML，Ws-Security

## 目錄

封面內頁 簽名頁 授權書.....	iii	中文摘要.....	v	ABSTRACT.....	v
.....vi 誌謝.....	vii	目錄.....	viii	圖目	
錄.....	xii	表目錄.....	xiv	第一章 緒論.....	1
背景.....	1	1.2 研究動機與目的.....	2	1.3 研究範圍與限制.....	3
第二章 文獻探討.....	4	2.1 SAML 文獻探討.....	4	2.1.1 OASIS 力	
推SAML.....	4	2.1.2 WS-Security .....	5	2.1.3 何謂SAML.....	5
身份驗證的確認.....	6	2.1.5 屬性的確認.....	6	2.1.6 授權決定的確	
認.....	6	2.1.7 SAML 之優點.....	7	2.2 B2B 網路交易.....	11
私密性.....	12	2.2.2 授權.....	12	2.2.3 資料完整性.....	12
訊息來源認證.....	12	2.2.5 不可否認性.....	12	2.3 SAML 安全認證機制在B2B 交易的應	
用.....	13	2.3.1 身份驗證的通訊協定.....	13	2.3.2 SAML 的認證模式.....	15
SAML 認證伺服器.....	16	2.4 相關安全標準機制說明.....	17	2.4.1 XKMS	
.....	17	2.5 XML 及XSLT 語法說明.....	18	2.5.1 XML.....	18
2.5.2 XSLT.....	19	第三章 研究方法與系統設計.....	24	3.1 SAML 安全認證機	
制.....	26	3.1.1 Schema Header and Namespace Declarations.....	26	3.1.3 Name Identifiers	
.....	27	3.1.4 Assertions .....	28	3.1.5 NotBefore 和 NotOnOrAfter 屬性.....	29
Statements .....	32	3.1.7 Attribute.....	35	3.1.8 SAML Protocols(SAML 協定)	
.....	37	3.2 採購系統設計.....	37	3.2.1 使用環境與開發工具.....	37
系統操作流程.....	37	3.3 基於SAML 之採購系統的安全性分析.....	39	3.3.1 XKMS 的規範及標	
準.....	40	3.3.2 XKMS 金鑰取得.....	51	3.3.3 SAML 之安全性分析.....	56
第四章 系統實作.....	62	4.1 安全採購作業流程.....	63	4.2 程式執行畫	
面.....	64	4.2.1 登入採購系統.....	64	4.2.2 採購系統程式執行畫面.....	64
4.2.3 系統參數設定.....	65	4.2.4 基本資料建檔.....	65	4.2.5 單據資料輸	
入.....	65	4.2.6 統計報表.....	66	4.2.7 帳務管理.....	66
單產生XML 流程.....	66	4.2.9 採購付款作業.....	71	4.3 討論.....	77
第五章 結論與建議.....	78	5.1 研究結論.....	78	5.1.1 SAML 機制保護B2B 交易安	
全.....	78	5.1.2 XML 及XLST 的特點.....	79	5.1.3 SAML 認證的優點.....	79
XKMS 與SAML 的特性相似.....	79	5.2 後續研究建議.....	79	參考文	
獻.....	81	圖目錄 圖 2 - 1 Microsoft 上網身份識別解決方案.....	9	圖 2 - 2 SAML 聯合網路身份	
識別.....	10	圖 2 - 3 SAML 需求者和供應者模型.....	14	圖 2 - 4 SAML 認證應用流	

程.....	16	圖 2 - 5 XSLT 資料處理模式.....	20	圖 2 - 6 XML 結合XSLT 瀏覽畫	
面.....	23	圖 3 - 1 研究流程圖.....	25	圖 3 - 2 SAML Request-Response Protocol .....	37
- 3 採購系統操作流程圖.....	38	圖 3 - 4 XKMS (SAML) Key Name、Key Value 註冊流程圖.....	42	圖 3 - 5	
XKMS(SAML)認證流程圖.....	43	圖 3 - 6 XKMS(SAML)註冊流程圖.....	45	圖 3 - 7 XKMS 金鑰取得	
註冊.....	51	圖 3 - 8 XKMS 產生Authentication Code .....	51	圖 3 - 9 XKMS 產生Key Name 及 Key Value	
.....	52	圖 3 - 10 XKMS 產生LOCATE 需求.....	54	圖 3 - 11 XKMS 送出LOCATE 需求.....	55
圖 3 - 12 XKMS 主機回應需求成功訊息.....	55	圖 3 - 13 SAML Single Sign-on 的瀏覽器與文件識別流程圖.....	57	圖 4 -	
1 基於SAML 之採購流程架構圖.....	62	圖 4 - 2 SAML 採購作業流程圖.....	63	圖 4 - 3 登入系	
統.....	64	圖 4 - 4 主程式執行畫面.....	64	圖 4 - 5 系統參數設定.....	65
4 - 6 基本資料建檔.....	65	圖 4 - 7 單據資料輸入.....	65	圖 4 - 8 單據資料輸	
入.....	66	圖 4 - 9 帳務管理.....	66	圖 4 - 10 報價單資料輸入.....	66
4 - 11 報價單轉XML .....	67	圖 4 - 12 報價單結合XSLT 瀏覽.....	70	圖 4 - 13 採購付款資料輸	
入.....	71	圖 4 - 14 採購付款資料轉XML 格式.....	72	圖 4 - 15 採購付款結	
合XSLT.....	75	表目錄 表 2 - 1 B2B 交易不同安全機制的比較.....	11	表 2 - 2 XML 宣告與文件種	
類.....	18	表 2 - 3 根元素.....	19	表 2 - 4 雜項.....	19
法架構.....	20	表 2 - 6 XML 內容.....	20	表 2 - 7 XSLT 內容.....	21
- 8 HTML 內容.....	22	表 3 - 1 Schema Header and Namespace Declarations .....	26	表 3 - 2 Simple Type	
DecisionType .....	27	表 3 - 3 Name Identifiers.....	27	表 3 - 4 NameIdentifier .....	28
- 5 EncryptedNameIdentifier .....	28	表 3 - 6 Issuer .....	28	表 3 - 7 AssertionIDReference NCName	
.....	29	表 3 - 8 AssertionIDReference AnyURI .....	29	表 3 - 9 Assertion.....	29
Conditions Type .....	30	表 3 - 11 AudienceRestrictionCondition.....	30	表 3 - 12 DoNotCacheCondition	
.....	31	表 3 - 13 ProxyRestrictionCondition .....	31	表 3 - 14 Advice.....	31
schema defined.....	32	表 3 - 16 Statement .....	32	表 3 - 17 SubjectStatement.....	
32 表 3 - 18 SubjectType .....	33	表 3 - 19 SubjectConfirmation .....	33	表 3 - 20	
AuthenticationStatement .....	34	表 3 - 21 SubjectLocality .....	34	表 3 - 22 AttributeStatement	
.....	34	表 3 - 23 AttributeDesignator.....	35	表 3 - 24 AttributeType .....	35
AttributeValue .....	35	表 3 - 26 AuthorizationDecisionStatement .....	36	表 3 - 27 Action	
.....	36	表 3 - 28 Evidence .....	36	表 3 - 29 系統使用之環境及開發工具.....	38
表 3 - 30 系統功能.....	39	表 3 - 31 SAML 與其他規範的關聯.....	40	表 3 - 32 Locate service	
.....	42	表 3 - 33 Locate Result .....	43	表 3 - 34 Validate Service .....	44
Validate Result .....	44	表 3 - 36 Reissue.....	45	表 3 - 37 Reissue Result.....	47
表 3 - 38 Revoke.....	48	表 3 - 39 Revoke Result .....	49	表 3 - 40	
Recover.....	49	表 3 - 41 Recover Result .....	50	表 3 - 42 KeyName 及Key Value	
.....	52	表 3 - 43 XKMS 主機回應XML 資料內容.....	56	表 4 - 1 報價單XML 內容.....	67
表 4 - 2 報價單XML 加密內容.....	68	表 4 - 3 報價單XSLT 內容.....	69	表 4 - 4 報價單網頁內	
容.....	70	表 4 - 5 採購付款XML 內容.....	72	表 4 - 6 採購付款XML 加密內容.....	
73 表 4 - 7 採購付款XSLT 內容.....	74	表 4 - 8 採購付款網頁內容.....	76	表 5 - 1 SAML 採購系	
統與傳統採購系統比較.....	78				

## 參考文獻

- [1] 張思源, 「Web服務安全標準及實務應用」, 民國92年 [2] 林以章, 「發展一企業間的電子商務系統模式 - 以物料需求計劃為例」, 大葉大學資訊管理系碩士論文, 民國89年 (指導教授:梁文耀 博士) [3] 李長庚, 「一個開放的WEB-based single sign-on 服務架構」, 國立交通大學資訊管理系碩士論文, 民國92年(指導教授:羅濟群 博士) [4] 潘士豪, 「關鍵鍊專案管理與全球資訊運籌系統」, 國立台灣大學機械工程系碩士論文, 民國92年(指導教授:陸一平 博士, 陽毅平博士) [5] Fabio Arciniegas 著, 張嘉麟 譯, 「XML 程式開發指南」, 民國91年, 麥格羅 希爾 [6] 陳燦煌 編著, 「Delphi 電子商務網站建構實務」, 民國90年, 博碩文化 [7] David Carlson 著, 小宇 譯, 「XML 與UML 整合開發實務」, 90年12月, 台灣培生教育出版股份有限公司 [8] 林錦雀, 江高舉 著, 「XML 基礎領航」, 民國92年4月, 金禾資訊股份有限公司 [9] 林胤良, 「企業間電子商務認證交換平台發展程序」, 南華大學資訊管理系碩士論文, 民國92年 (指導教授:吳光閔 博士) [10] 陳志昌編譯, 「UML 技術手冊」, 民國90年, 美商歐萊禮股份有限公司台灣分公司。譯自UML in a Nutshell, 原著 Alhir,S. S.
- [11] OASIA, <http://www.oasis-open.org>,[SAML Version 2.0 Scope and -Work Items], 7 November 2003.
- [12] XML台灣資訊網, <http://www.xml.org.tw> (2004.6.30) [13] Tae-Sun Chung, Hyoung-Joo Kim, [Techniques for the evaluation -of XML queries: a survey], Data & Knowledge Engineering 46(2003) 225 – 246 [14] Thomas Gros IBM Zurich Research Laboratory Security Analysis -of

the SAML Single Sign-on Browser / Artifact Profile, IEEE2003 [15] OASIS SAML Interoperability Event Demonstrates Single Sign- -On at RSA Conference <http://xml.coverpages.org/ni2004-02-19-a.html> (2004.6.30) [16] TestMaker <http://www.pushtotest.com/ptt/books/thebook.html>(2004.6.30) [17] Web Services Security (WS-Security) [http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnglobspec/html/wssecurity.-asp#ws-security\\_\\_toc6120228](http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnglobspec/html/wssecurity.-asp#ws-security__toc6120228) (2004.6.30) [18] Imamura, Takeshi, et al., " XML Encryption Syntax andProcessing , " W3C, 2002/3 [19] Moses, Tim and Prateek Mishra, et al., " Security and Privacy -Considerations for the OASIS Security Assertion Markup -Language (SAML), " Organization for the Advancement of -Structured Information Standards(OASIS), 2002/4 [20] 瞭解 ws - security <http://www.microsoft.com/taiwan/msdn-/library/2002/Nov-2002/understw.htm> (2004.6.30) [21] 網際網路交易安全 <http://www.taica.com.tw/education/ca-1-1.htm> (2004.6.30) [22] 網際網路加強安全把關 WS-Policy <http://taiwan.cnet.com/-news/story/0,2000022589,20061608,00.htm> (2004.6.30) [23] SSL 不足以提供電子商務安全 <http://taiwan.cnet.com/news/-software/0,2000064574,20083409,00.htm> (2004.6.30) [24] XML 加密標準 ( W3C XML Encryption , 簡稱XMLEnc ) - <http://www.w3.org/TR/xml-encryption-req> (2004.6.30) [25] 身分驗證及權限控制的SAML 標準 ( OASIS Security -Assertions Markup Language , 簡稱SAML ) , <http://www.oasisopen.-org/committees/security/#documents> (2004.6.30) [26] 管理存取權限的XACML 標準 ( OASIS Extensible Access -Control Markup Language ) , <http://www.oasisopen.-org/committees/xacml> (2004.6.30) [27] 取代PKI 來管理公開金鑰的XKMS 標準, XML 金鑰管理規範 ( XML Key Management Specification , 簡稱XKMS ) , <http://www.oasis-open.org/cover/xkms.html> (2004.6.30) [28] XML 加密語法處理規範 <http://www.w3.org/TR/2002/RECxmenc-core-20021210/> , XML Encryption Syntax andProcessing (2004.6.30) -Schema: <http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-schema.xsd> (2004.6.30) -Example: <http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/enc-example.xml> (2004.6.30) [29] XML 簽章解密轉換標準 <http://www.w3.org/TR/2002/RECxmle-nc-decrypt-20021210> (2004.6.30) [30] OASIS 的Web 服務安全技術委員會 [http://www.oasisopen.org/committees/tc\\_home.php?wg\\_abbrev=wss](http://www.oasisopen.org/committees/tc_home.php?wg_abbrev=wss) (2004.6.30) [31] OASIS WEB SERVICE SECURITY:SAML Token Profile -Working Draft 09,27 January 2004 [32] Computerworld SAML Secures Web Services : - <http://www.computerworld.com/developmenttopics/development/-webdev/story/0,10801,73712,00.html> (2004.6.30) [33] Computerworld SAML's Cousin: WS-Security - <http://www.computerworld.com/developmenttopics/development/-webdev/story/0,10801,73662,00.html> (2004.6.30) [34] 數位認證:該用Liberty 或Passport ? John Pescatore and -Avivah Litan/Gartner 陳爽總譯 2003/11/19 - <http://taiwan.cnet.com/enterprise/technology/0,2000062852,20085635,00.htm> (2004.6.30) [35] 黃崇德, 「 XML 導入與產業電子化XML Key Management -Specification ( XKMS 2.0 ) 」 , 中原資管所, 民國93 年 [36] Article Single Sign-on Simplicity with SAML May 9, 2002 <http://java.sun.com/features/2002/05/single-signon.html>(2004.6.30) [37] XML Key Management (XKMS 2.0) Requirements <http://www.w3.org/TR/xkms2-req> (2004.6.30) [38] 澄清 SAML 的不實說法 and 誤解 <http://www-900.ibm.com/-developerWorks/cn/xml/x-samlmyth/index.shtml#11> (2004.6.30) [39] XML 測試網站 [http://www.w3schools.com/xml/xml\\_](http://www.w3schools.com/xml/xml_) <http://taiwan.cnet.com/news/software/0,2000064574,20073844,00.htm> (2004.6.30) [40] Taiwan.cnet.com 科技資訊網 微軟連夜彌補Passport 安全漏洞