

A Single Sign-on Scheme for Web Services Based Multinational Enterprise Information Systems Using Smart Cards

張清爽、曹偉駿

E-mail: 9808373@mail.dyu.edu.tw

ABSTRACT

With the trend of internationalization, multinational management has become an important issue for multinational enterprises. Thus, how to add the functionality of re-resource sharing causes a noticeable challenge. However, all personnel of enterprises will feel inconvenient when they access to the data among branch offices due to a huge mass of loose database systems, heterogeneous platforms, and inconsistent authority problems. Therefore, we solve the limits of user authentication across different system environments by employing web services architecture, then accomplish the capability of single sign-on by following security assertion markup language (SAML) standard, and further integrate smart card technology, in order to effectively enhance system security. Finally, our study implements a multinational enterprise information system to verify the proposed scheme, and also makes comparisons with current approaches, so that we can sufficiently demonstrate the contributions of our proposed scheme, including saving large number of communication costs, satisfying security requirements of information system, and so on.

Keywords : web services、 security assertion markup language、 single sign-on、 smart card

Table of Contents

中文摘要	iii
英文摘要	iv
誌謝辭	v
內容目錄	vi
表目錄	viii
圖目錄	ix
第一章 緒論	1
第一節 研究動機與背景	1
第二節 研究目的	2
第三節 研究流程	3
第四節 論文架構	5
第二章 文獻探討	6
第一節 智慧卡	6
第二節 網路服務	10
第三節 單一登入	14
第四節 小結	19
第三章 研究方法	21
第一節 註冊階段	22
第二節 登入階段	23
第三節 取得服務階段	24
第四節 系統流程	25
第四章 系統建置與分析	26
第一節 系統規格	26
第二節 系統實作與測試	27
第三節 安全性分析	32
第四節 效能與分析	34
第五章 結論與未來發展	37
參考文獻	38

REFERENCES

一、中文部份陳清裕(2001), 國民身分證IC卡安全規劃與可行性研究, 私立淡江大學資訊管理學系未出版之碩士論文。張群(2002), 微軟?位憑證機制與智慧卡之整合與運用-以校園?位憑證系統為?, 私立樹德科技大學資訊管理研究所未出版之碩士論文。二、英文部份Alvin, T. S., & Dicj, K. T. (2005). Web services mobility in a pocket. Proceedings of IEEE International Conference on ICWS (pp. 159-166), USA: Orlando, Florida. Beznosov, K., & Flinn, D. J. (2005). Shirley Kawamoto, Bret Hartman, introduction to web services and their security. Information Security Technical Report, 10(1), 2-14. Chuvakin, A. & Peterson, G. (2009). Logging in the age of web services. IEEE Security & Privacy, 7(3), 82-85. Clercq, J. D., & Grillenmeier, G. (2007). Microsoft Windows Security Fundamentals. USA: Butterworth-Heinemann, 533-579. Dang, L., Kou, W. & Xiao, Y. (2005). An improved scheme for unilateral asymmetric smart card authentication. IEEE Advance information Networking and applications, 2(5), 265 -268. Gammel, B. M. & Inside S. J. (2005). Smart Card Inside. Proceedings of European Solid-State Device Research Conference (pp.69-74), Grenoble, France. Gudivada, V. N. & Nandigam, J. (2005). Enterprise application integration using extensible web services. Proceedings of the IEEE International Conference on Web Services(pp.41-48), USA: Washington, District of Columbia. Harikumar, A. K., Lee, R., Yang, S. H., Kim, H. K., & Kang, B. (2005). A model for application integration using web services. Proceedings of Computer and Information Science Fourth Annual ACIS International Conference(pp.468-475), Jeju Island, South Korea. Hansen, S. M., Skriver J., & Nielson, H. R. (2005). Using static analysis to validate the SAML single sign-on protocol. Proceedings of ACM workshop on Issues in the theory of security (pp.27-40), Long Beach, California. Juang, W. (2005). Efficient Multi-server password authenticated key agreement using smart cards. IEEE Transactions on Consumer Electronic, 50(1), 251-255. Kerschbaum, F., & Robinson, P. (2009). Security architecture for virtual organizations of business web services. Journal of System Architecture, 55(4), 224-232. Kardas, G., & Tunali, E. T. (2006). Design and implementation of a smart card based healthcare information system. Computer Methods and Programs in Biomedicine, 8(1), 66-78. Lu, R., & Cao, Z. (2005). Efficient remote user authentication scheme using smart card. Computer Networks, 49(5), 535-540. Nobayashi, D., Nakamura, Y., Ikenaga, T., & Hori, Y. (2009). Development of Single Sign-On System with Hardware Token and Key Management Server. IEICE TRANSACTIONS ON INFORMATION AND SYSTEMS, E92D(5), 826-835. Patrick, Y. K. Chau. (2003). Octopus: An E-cash payment system success story. Communication of ACM, 46(9), 129-133. Renaudin, M., Bouesse, F., Proust, Ph., Tual, J. P., Sourgen, L., & Germain, F. (2004). High security smartcard. Proceedings of the Design, Automation and Test in Europe Conference and Exhibition (pp. 228-232), Grenoble, France. Satoh, F., & Itoh, T. (2004). Single sign on architecture with dynamic tokens. Proceedings of the 2004 International Symposium on Applications and the Internet (pp.197-200), Tokyo, Japan. Sanchez, M., Lopez, G. C. Novas, J. & Antonio, F. (2009). Performance analysis of a cross-layer SSO mechanism for a roaming infrastructure. Journal of Network and Computer Applications, 32(4), 808-823. Shaer, C. (1995). Single sign-on. Network Security, 1995(8), 11-15. Tiri, K. (2005). Design method for constant power consumption of differential logic circuits. Proceedings of the IEEE Design, Automation and Test in Europe Conference and Exhibition(pp. 628-633), Messe Munich, Germany. Tsaor, W. J. & Lin, Y. M. (2009). An agent-based single sign-on Scheme for web services environments. Proceedings of the 2009 International Conference on Security and Management (SAM ' 09), Las Vegas, USA. Yoon, E., & Yoo, K. (2005). More efficient and secure remote user authentication scheme using smart cards. Proceedings of the IEEE Parallel and Distributed 11th International conference (pp.73-77), Fukuoka, Japan.