International Journal of Innovative Computing, Information and Control
Volume **6**, Number **11**, November **2010**

ICIC International ©2010 ISSN 1349-4198
pp. 5259–5274

SMART CARD-BASED SECURE WEB SERVICES IN THE THREE-PARTY SETTING

Ren-Chiun Wang[1], Wen-Shenq Juang[2] and Chin-Laung Lei[1,*]

[1]Department of Electrical Engineering
National Taiwan University
No. 1, Sec. 4, Roosevelt Rd., Taipei 106, Taiwan
rcwang@fractal.ee.ntu.edu.tw
*Corresponding author: lei@cc.ee.ntu.edu.tw

[2]Department of Information Management
National Kaohsiung First University of Science and Technology
No. 2, Jhuoyue Rd., Nanzih District, Kaohsiung 811, Taiwan
wsjuang@ccms.nkfust.edu.tw

Received July 2009; November 2009

Abstract. *Going along with the rapid development of web technologies, people can make a great quantity of transactions through web services. For some purpose-restricted applications, service requesters and service providers locate at different network domains and they want to protect their delivery contents against being eavesdropped, altered, or fabricated from outsiders. They require a communal trusted third party to help them achieve the purpose. Using a traditional two-party key agreement protocol to negotiate a common session key in three-party case, the communication and computation cost are high. In this paper, we propose a three-party key agreement protocol to construct a secure communication for web services using smart cards. In our protocol, the major merits include: (1) prevention of the replay attack; (2) satisfaction of the perfect forward secrecy; (3) satisfaction of the master key forward secrecy; (4) prevention of the password guessing attack; (5) satisfaction of the explicit key confirmation; (6) prevention of the impersonation attack; (7) security against the session state reveal; and (8) prevention of the smart card loss problem.*

Keywords: Authentication, Password, Random oracle model, Smart card, Three-party key agreement

1. Introduction.

Today, people have many opportunities to delivery their service requests to service providers through public networks, where the purposes of the requests may be for individuals, businesses or governments [8, 15, 21]. The contents of the delivery service could be sensitive information and both of the service requester and the service provider are distributed over different network domains [32]. First, they require a communal trusted third party to help them with agreeing an encryption key. Then the web service mechanism must provide a solution to eliminate unauthorized parties from eavesdropping the delivery contents. We use a scenario in an e-government to explain it. When the Criminal Investigation Bureau (CIB) wants to investigate the flow of financial affairs in a bank for someone. The CIB sends the request to the bank. The CIB plays the role of a service requester and the bank plays the role of a service provider. However, they do not trust each other over the Internet. Now, the Financial Supervisory Commission (FSC) acts a broker and is trusted by the CIB and the bank. The FSC becomes a bridge to help the CIB and the back to establish a secure channel for delivering the service. Consider another scenario for the individuals, a purchaser may purchase some goods from