International Journal of Innovative Computing, Information and Control
Volume **7**, Number **6**, June **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 3097–3106

AN EFFICIENT MUTUAL AUTHENTICATION PROTOCOL FOR RFID SYSTEMS

Iuon-Chang Lin[1,*], Chi-Wei Wang[2], Rui-Kun Luo[2] and Hsin-Chiang You[3]

[1]Department of Management Information Systems
National Chung Hsing University
No. 250, Kuo Kuang Road, Taichung 402, Taiwan
*Corresponding author: iclin@nchu.edu.tw

[2]Department of Computer Science and Information Engineering
Asia University
No. 500, Lioufeng Road, Wufeng, Taichung 41354, Taiwan

[3]Department of Electronic Engineering
National Chin-Yi University of Technology
No. 35, Lane 215, Sec. 1, Chung-Shan Road, Taiping City, Taichung 41101, Taiwan

Received April 2010; revised August 2010

Abstract. *After the world's largest retailer, Wal-Mart, has implemented RFID (Radio Frequency Identification), the global suppliers are actively devoted to EPC (Electronic Product Code) research and development. Since RFID has advantages of a long life, safe and free from environmental constraints, RFID EPC can achieve benefits such as saving manpower costs, expressing logistics management, reducing man-made orders and decreasing excess inventory. The paper is to explore the security issues of the RFID EPC Class 1 Generation 2. RFID transmits information wirelessly, therefore, information can be captured. In order to protect data privacy, many scholars have proposed their own ways to improve. This paper has extended the scheme of Duc et al., and made a more efficient version.*

Keywords: RFID, EPCglobal, Mutual authentication, Security, MAC

1. Introduction.

1.1. RFID introduction.

RFID is a tiny electronic tag attached to the items. By radio identification technology, RFID system can identify electronic tag and send data to the back-end host to achieve tracking, verification and control [7]. It is a non-contact automatic identification technology.

RFID system consists of three parts:

- **Tag:** used to store information on electronic merchandise.
- **Reader:** used to read electronic tags by using RF signals so that reader does not require making contact with tags to read. Reader connected with the computer will read the information of tag, and sends information back to the back-end host for identification and the follow-up treatment.
- **Back-end server:** used to process the information sent by reader and verify the legitimacy of tag.

The architecture can refer to Figure 1.

RFID tag can be divided into three categories in accordance with its own power supply:

- **Active tag:** This tag itself powered by a battery that can repeat read/write with memory more than 1MB and has long transmission distance. The disadvantage is bulky, and the batteries need to be replaced and are very expensive.