Security Scheme for Managing a Large Quantity of Individual Information in RFID Environment

Namje Park

Department of Computer Education, Teachers College, Jeju National University,
61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, Korea
namjepark@jejunu.ac.kr, namjepark@gmail.com

Abstract. Mobile RFID environment means that mobile RFID devices like mobile (cellular) phone and PDA employing cellular network can be used at querying information of the consumer product related a tag. The mobile RFID devices should have mobile RFID readers which are made for them and are, in particular, compliant with EPC Class-1 Generation-2 UHF (860-960 MHz) standard. Ensuring the security of mobile RFID's large-capacity database system by depending only on existing encryption schemes is unrealistic. In this paper, we propose a security service solution for managing a large quantity of individual information in mobile RFID environment. It aims to become aware of distribution of large quantity of individual information with RFID tags and to provide information service to general consumers with mobile RFID devices like mobile phone or PDA which has a mobile RFID.

1 Introduction

Radio Frequency Identification (RFID) technology is being actively developed to exploit its global market potential. At the same time, it has raised fears among those who believe that it could facilitate a 'Big Brother' society. Thus, technology development efforts in areas such as tags, readers, and middleware should address not only information and market needs but also privacy and security concerns. The excessive limitations of RFID tags and readers have made it impossible to apply present codes and protocols. Technologies for information and privacy protection should address the general interconnection among elements, and their RFID characteristics should closely reflect the RFID environment.

Common RFID technologies have been used in B2B (business to business) models (e.g., supply channel, distribution, and logistics management), whereas mobile RFID technology have been used in the RFID reader attached to an individual owner's mobile phone, through which the owner can collect and use information on objects by reading their RFID tags. Corporations have applied mobile RFID technologies mainly to B2C (business to customer) models for marketing. Although RFID services have been limited largely to fields requiring less security (e.g., searching for movies and providing information in galleries), such services are expected to be applied more extensively to fields that necessitate privacy and security (e.g., purchasing, healthcare, and electrical drafts).

R. Zhu et al. (Eds.): ICICA 2010, Part II, CCIS 106, pp. 72–79, 2010.

The secure storage and management of RFID's personal data has become an important issue, leading to the encryption of data to address security threats. However, the encryption scheme requires a lot of time and memory for encoding and decoding. Because encryption schemes such as the Advanced Encryption Standard (AES) encode confidential information in its entirety, there is a risk of the outflow of entire information once the secret key is decoded; hence, the distribution and management of the key is difficult. Unlike the encryption scheme, there is no such thing as the life of a key under the secret sharing scheme; thus, secret sharing scheme presents no problems in terms of public key certificate-based authentication and can substantially reduce operational costs. By contrast, under the existing secret sharing scheme, if original data are separately stored, the size of share (i.e., distributed information) equals that of the original data, increasing the data volume to be stored. Recently, it has been found that transforming the plaintext (in the encryption mode) before encoding improves data security while maintaining the efficiency of the existing encryption scheme.

In this paper, we propose a security service solution for managing a large quantity of individual information in mobile RFID environment. It aims to become aware of distribution of large quantity of individual information with RFID tags and to provide a information service to general consumers with mobile RFID devices like mobile phone or PDA which has a mobile RFID.

2 Related Research

2.1 Networked Mobile RFID Technology

RFID is expected to be the base technology for ubiquitous network or computing, and to be associated with other technology such as telemetric, and sensors. The mobile phone integrated with RFID can activate new markets and end-user services, and can be considered as an exemplary technology fusion. Furthermore, it may evolve its functions as end-user terminal device, or 'u-device (ubiquitous device)', in the world of ubiquitous information technology.

Networked mobile RFID means an expanded RFID network and communication scope to communicate with a series of networks, inter-networks and globally distributed application systems. So it makes global communication relationships triggered by RFID, for such applications as B2B, B2C, B2B2C, G2C, etc. Networked mobile RFID loads a compact RFID reader in a cellular phone, providing diverse services through mobile telecommunications networks when reading RFID tags through a cellular phone. Internet-enabled mobile phone which equips RFID reader will bring new service concepts to mobile telecommunication.

Networked mobile RFID technology is focusing on the UHF range (860~960MHz), since UHF range may enable longer reading range and moderate data rates as well as relatively small tag size and cost. Then, as a kind of handheld RFID reader, in the selected service domain the UHF RFID phone device can be used for providing object information directly to the end-user using the same UHF RFID tags which have widely spread. The service area of networked mobile RFID is expected to be unlimited, and its services, diverse; currently, however, the service scenarios using