Chapter 8
A Methodology for UICC-Based Security Services in Pervasive Fixed Mobile Convergence Systems

Jaemin Park
Convergence WIBRO BU, KT (Korea Telecom), Republic of Korea

ABSTRACT

Nowadays, Fixed Mobile Convergence (FMC) is an emerging worldwide trend in the form of fixed and mobile telephony convergence. In this pervasive environment, security should be considered to be a more important factor than before because the security threats of heterogeneous infrastructures can happen simultaneously. Thus, UICC, the ideal and secure medium embedded on the mobile terminals, has been utilized to provide the security-sensitive services and the service security framework of the mobile terminals.

This chapter presents the fundamental and security characteristics of UICC and current practices of UICC-based security services (e.g. banking, stock, network authentication, etc.) in pervasive FMC systems. Moreover, we propose a novel UICC-based service security framework (USF), which implements the essential security functionalities used for FMC services, to provide the integrated security infrastructure and secure FMC services. The USF can be utilized to authenticate users, preserve privacy, and protect network infrastructures and business models of telephony companies.

INTRODUCTION

The FMC is a worldwide and clear trend in the form of fixed and mobile telephony convergence. The aim of the convergence between fixed and mobile telephony is to provide both services with a dual mode terminal. In this pervasive environment, the security should be considered as an important factor since the security threats of fixed and mobile networks and service infrastructures can be happened simultaneously. Most FMC services should necessitate personal sensitive

DOI: 10.4018/978-1-60960-735-7.ch008

information like ID/Password, certificates, bank accounts, credit card numbers, etc. Moreover, a single terminal can be used among different kinds of network and service infrastructures, which need an individual security protocol. Therefore, the integrated security infrastructure of the mobile terminal should be mandatory.

The trend of openness in the FMC environment can bring about more fatal security threats, for examples, leakage of private information, phishing, mobile viruses, etc. Accordingly, customers' interests in the security have been increased drastically to preserve their privacies and information. Telephony companies also would like to comply with customers' security requirements and protect their network infrastructures and business models against various threats.

Since the mobile terminals should be the endpoints of mobile services and storages of personal information, the security of terminals must be important for secure FMC services. However, due to the inevitable constraints of the mobile terminals such as lack of hardware-based crypto processor, insecure memories, etc., fully secure FMC services had seemed to be difficult.

Nowadays, UICC has been deemed to be the only solution to address the security issues of the mobile terminals due to the brilliant advances in technologies of the smartcards. Moreover, UICC is owned and controllable by mobile operators and is therefore more flexible than mobile terminals in providing security according to the security requirements of services and can be inserted in any terminal regardless of its base operating system.

In this chapter, we present methodologies for UICC-based security service in pervasive FMC systems. We briefly explain the fundamental and security characteristics of UICC and present current practices of UICC-based security services. Then, UICC-based Service Security Framework (USF) is proposed and its practices are explained. Finally, we describe the future research direction and conclude this chapter.

BACKGROUND

The UICC is the smartcard used in mobile terminals in GSM and UMTS networks. The UICC can guarantee the integrity and security of the personal data such as the phone number, messages, contact information (phonebook, e-mail, etc.) and so forth. SIM and USIM applications acting as the user authentication modules are stored in the UICC, respectively for GSM and UMTS networks. When the mobile terminals are starting to be activated, SIM and USIM applications begin to operate the authentication procedures with AuC (Authentication Center). For this, these applications and AuC should share the secret key for user authentication. These applications are the fundamental and most important among other applications in the UICC.

Several applications for UICC value added services can be stored in the memory such as EEPROM, flash, etc. of the UICC. Most of these applications can be pre- or post- loaded, installed and instantiated based on the GlobalPlatform, the UICC management platform for the issuers. These applications are usually implemented on top of the Java Card Platform, which provides the java card runtime environment, java virtual machine and APIs. The applications mostly facilitate the APIs to invoke the methods supported by Java Card Platform. The examples of these applications can be transportation, banking, stock, credit card, loyalty, etc. Most of these services are utilizing the security characteristics of UICC and further explained in the following chapters.

The applications installed on the UICC can be further categorized as the applets and the servlets. The applet is a simple Java card application without UI and communicates with the off-card entities via APDU ((Application Protocol Data Unit), which is the communication unit defined in ISO/IEC 7816-4. For the clarity, we'd like to explain more about the APDU. Two kinds of APDUs are existed: command APDUs and the response APDUs. A command APDU is sent by the off-card entity to the UICC and should contain a 5-byte header