Security Models for High Capacity USIM-based Services

Eun Su Jeong[1], Bum Han Kim[2], and Dong Hoon Lee[3], *, Member, IEEE

Korea University, Center for Information and Security Technologies (CIST),
Anam Dong, Sungbuk Gu, Seoul, Korea
eunsu.jeong@sk.com[1], i.bhkim@gmail.com[2], donghlee@korea.ac.kr[3], *

Abstract. As the USIM technologies are evolving to include high speed CPU, mass storage devices, and high speed serial interfaces, various services are to be available through those technologies. The high capacity USIM card is a combination of IC card and high capacity flash memory. Because the flash memory does not provide security, additional protection technologies need to be incorporated for privacy issues and data protection. In this paper, we defined the security models for each service that can be provided from high capacity USIM card. Consequently, the results of this study are expected to be widely applied to development of high capacity USIM and the related commercial services as a foundation technology or references.

Keywords: High Capacity USIM, Security Model, Smart Card.

1 Introduction

A high capacity USIM card consists of an IC card and a flash memory. Accordingly, it can offer both securability and applicability. To store specific data on a limited USIM card, the flash memory can be used. However, since the flash memory does not provide securability, additional security features such as privacy should be included in the data that relates to various services.

In this paper, we suggested the security models with service area and smartcard area respectively in the high capacity USIM. For each security model, we defined the features and purposes for each entity in the high capacity USIM, illustrated the trusted relationship between entities, and compared the service examples and features between security models.

In Section 2, we analyzed the technical features of the high capacity USIM and smartcard-based security schemes. The security models in USIM-based service are defined in Section 3. Lastly, Section 4 summarizes the paper.

2 Related Work

2.1 Overview of high-capacity USIM

The high capacity USIM card is a more advanced type of the USIM with limited resources and it provides high performance CPU, mass storage, and high speed interfaces.

Firstly, The USIM card provides a trusted security. The embedded smart card can securely protect data different from other embedded and external memories. In addition, it contains the cryptographic coprocessor to efficiently perform arithmetic operations.

Secondly, once users own their USIM cards, because they must use them for a long time, users can securely manage their own content and privacy through USIM cards.

2.2 Security schemes using smartcard

Hwang et al. [1] proposed a remote user authentication scheme using smart cards. In 2002, Chien et al. [2] proposed an efficient password based remote user authentication scheme, and claimed that their scheme has the merits of providing mutual authentication. Lee at al. [3] proposed an improvement to Chien et al.'s scheme to prevent parallel session attack. Yoon et al. [4] claimed that the scheme using previously generated secret hash values are secure even if the secret key of the system is leaked or stolen and users can update their passwords freely and securely. Liaw et al. [5] proposed a remote user authentication scheme using smart cards. Conrado et al. [6] proposed the smartcard-based DRM system. Accordingly, Sun et al. [7] proposed a resolution protocol. Their theses are mainly focused on the architectures for smartcard-based DRM systems to make up for the weak points of the device-based DRM systems.

However, the security architecture to implement various services using the high capacity USIM card has not been studied yet. In this paper, we established the security models for individual high capacity USIM-based services.

3. Security Models

In this Section, we focus on the service-related security model in the service domain area. The trusted relationship structure defines whether or not to trust other entities. The purpose of this structure is to securely maintain various contents and data and to define the trusted relationship between entities.

Consequently, according to the service domain and used security technology, the models are subdivided into the basic security model, external security model, asymmetric security model, and public security model [Fig. 1].

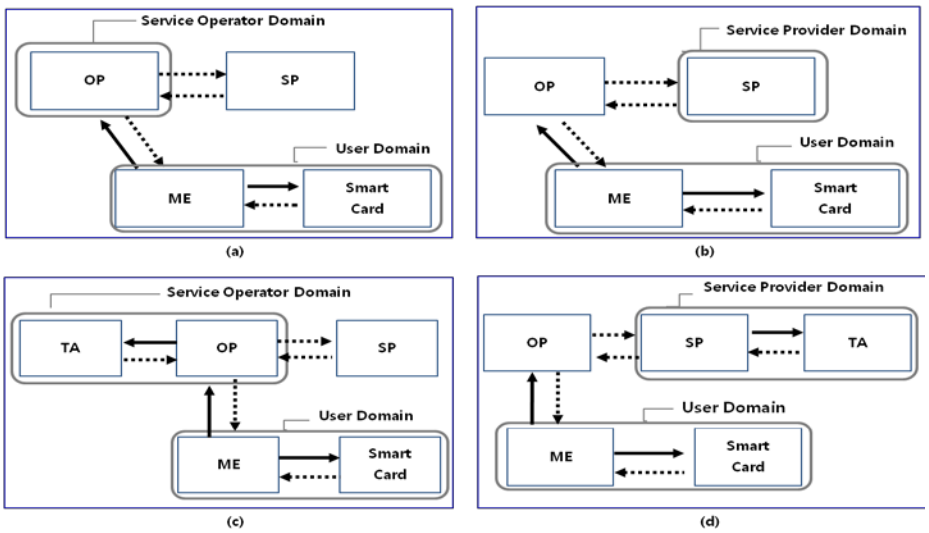

Fig. 1. Trusted Relationship between Entities for Security Models (a: Basic Security Model, b: External Security Model, c: Asymmetric Security Model, d: Public Security Model)

The related terms and symbols are as follows:

Table 1. Terms and Symbols

Term/Symbol	Description
OP (Operator)	Service operator: Operator that provides mobile services
SP (Service Provider)	Service provider: Agency that provides value-added services through mobile networks
TA (Trust Authority)	Trust authority: Management agency that can be trusted. Its role may differ according to the platform technology.
ME (Mobile Equipment)	Terminal or mobile device while in use of mobile communication services
A ⟶ B	Entity A trusts Entity B
A ⇢ B	Entity A does not trust Entity B.

The basic security model is applied to internal services in the mobile operator that are similar to the USIM applications that authenticate subscribers and perform key exchange and encryption in the mobile zone.

In the external security model, the service provider generates the secret key. Accordingly, the management of keys is very important for business confidentiality. For instance, in the general purpose e-money service, even the service provider must not know the secret keys.

Both the asymmetric security model and public security model are all based on PKI. PKI uses the public key cryptography algorithm and the trusted agency (TA) generates the certificate for verification of the public key.

In this study, we suggested four different security models concerning the technologies and services that use high capacity USIM cards. Actually, four different security models are partly applied in specific fields. Thus, we designed those models flexibly to meet the technology and service requirements.

4. Conclusion

In this paper, we proposed security models for high capacity USIM-based services. The security models are applied to basic model, external model, asymmetric model, and public model. Each security model has been designed considering the USIM card technologies, services, and future scalability.

The suggestions are optimized only for security requirements so they have been designed to add the service-oriented communication protocols and procedures into commercial services. Consequently, the results of this study are expected to be widely applied to development of high capacity USIM and the related commercial services as a foundation technology or references.

Acknowledgments This research was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2012-0006419)

References

1. Hwang, M.S., Li, L.H.: A new remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, pp. 28-30 (2000)
2. Chien, H.Y., Jan, J.K., Tseng, Y.M.: An efficient and practical solution to remote authentication: smart card. Computers & Security, vol. 21, no. 4, pp. 372-375 (2002)
3. Lee, S.W., Kim, H.S., Yoo, K.Y.: Improved efficient remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp.565-567 (2004)
4. Yoon, E.J., Yoo, K.Y.: More Efficient and Secure Remote User Authentication Scheme using Smart Cards. In: Proc. of 11th International Conference on Parallel and Distributed System, vol. 2, pp. 73–77 (2005)
5. Liaw, H.T., Lin, J.F., Wu, W.C.: An efficient and complete remote user authentication scheme using smart cards. Mathematical and Computer Modeling, vol. 44, pp. 223-228 (2006)
6. Conrado, C., Kamperman, F., Schrijen, C. J., Jonker, W.: Privacy in an Identity-based DRM System. In Proceedings of the 14th IEEE Int.Workshop on Database and Expert Systems Applications, pp.389-395 (2003)
7. Sun, H.M., Hung, C.F., Chen, C.M.: An Improved Digital Rights Management System Based on Smart Cards. Proc. of the International Conference on Digital EcoSystems and Technologies,Cairns, Australia, pp. 308-313 (2007)