Security Scheme for High Capacity USIM-based Services

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

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 and proposed eligible architectures and security schemes for internal storage of the smartcard. 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, Secure Storage, Smart Card*

1. Introduction

USIM card, a core element of 3G mobile communication technology, is providing unique functions for key exchange and authentication upon network access. Recently, as the technologies are evolving including high speed CPU, mass storage devices, and high speed serial interfaces, various services that were not necessary in the past become mandatory. Especially, while the device-based structures are moving toward the USIM-centric structures concerning the USIM lock, various security issues are being raised.

A high capacity USIM card has an IC card and a flash memory together. Accordingly, it can offer both securability and applicability. To store specific data on the limited USIM card, the flash memory is used. However, since the flash memory does not provide security, additional security features such as privacy must be included for the data relating 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.

The protected areas using the internal secure storage in the high capacity USIM are subdivided into three areas (system, service, and user areas). For each area, we proposed the secure architectures, key management, and cryptography protocols for future use in high capacity USIM designs and commercial services.

The remainder of this paper is organized as follows. 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. In Section 4, we proposed the internal secure storage architectures and cryptography schemes for the high capacity USIM. Lastly, Section 5 summarizes the paper.

2. Related Work

This section gives an overview of high-capacity USIM and existing security schemes using smart card.

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. This feature of the USIM card does not simply mean the performance increase. Because the card provides the management features for services and personal privacy, it can also provide various functions that have been provided by terminals.

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. Accordingly, from the developer point of view, the privacy function is easily added in newly developed applications. So users can trust the data.

Secondly, once users own their USIM cards, because they must use them for a long period of time, users can securely manage their own contents and privacy information through USIM cards. Accordingly, this feature enables us to expand business opportunities by including various services in USIM cards.

As shown in Figure 1, the high capacity USIM contains 32-bit CPU, EEPROM, RAM, memory controller, and flash memory. It also provides interfaces to ISO, MMC, and USB for communication with the host application.

The advantages of high capacity USIM are as follows:

Table 1. Comparison between High Capacity USIM Card and Other Storage Devices

Memory Type	(U)SIM	Flash Memory	High Capacity USIM
Advantage	- Secure - Controllable	- Large storage - Can support multimedia services - Can support high speed interfaces - Multimedia-based GUI	- Compatible - Large storage - Can support high speed interfaces - Securability
Disadvantage	- Slow interface - Limited storage - Text-based GUI	- No securability - No controllability	

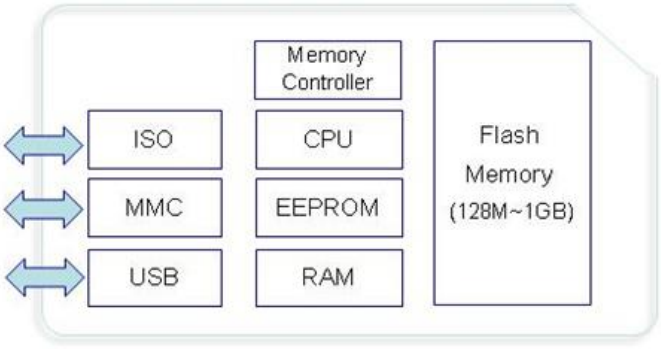

Figure 1. Structure of High Capacity USIM

2.2 Security schemes using smartcard

As the network data volume and usage are increasing, the data security gets more important due to increase of network-based intrusions and attacks.

Hwang *et al.*, [1] proposed a remote user authentication scheme using smart cards. Sun [2] proposed an efficient and practical remote user authentication scheme using smart cards. The proposed scheme reduces the communication and computation costs compared to Hwang *et al.*, [1]. In 2002, Chien *et al.*, [3] proposed an efficient password based remote user authentication scheme, and claimed that their scheme has the merits of providing mutual authentication, allowing users to freely choose the password, requiring no verification table, and involving only a few hashing operations. Lee *et al.*, [4] proposed an improvement to Chien *et al.*'s scheme to prevent parallel session attack. Yoon *et al.*, [5] 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.*, [6] proposed a remote user authentication scheme using smart cards. Using the proposed scheme, users can freely choose their passwords for change, requiring no verification table.

Conrado *et al.*, [7] proposed the smartcard-based DRM system. Once a license is purchased, users can utilize the contents anytime, anywhere, and from any devices. However, the protocol proposed by Cornardo *et al.*, does not encode the digital content so unprivileged users can access the content and the role of content provider is ambiguous. Accordingly, Sun *et al.*, [8] 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.

Trampus *et al.*, [9] proposed the scheme to store digital signature added documents and properly manage them. It allowed the increase of smartcard usability and e-business reliability.

In Hughes *et al.*, [10], smart cards were used for authentication of individual users to the Secure File System. While being used as a core element of SFS, the SFS structure was securely designed.

If we look at the security schemes using smartcards, the studies on the remote authentication and DRM key management based on smartcard's security stability and portability are progressing well. Furthermore, the schemes to securely store and manage

electronic documents have been studied. 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 and studied the schemes to utilize the memory area in the high capacity USIM as a secured storage.

3. Security Models

In this study, the security models are defined as follows. The security model defines the functions and purpose of entities in high capacity USIM card application environment and establishes the trusted relationship between entities. Thus, we can describe which security technology needs to be applied between entities through the security model. In this study, we defined the security model that reflects the high capacity USIM smartcard technology and services. As shown in Figure 2, the proposed security model consists of the security models for service domain and smartcard domain [11].

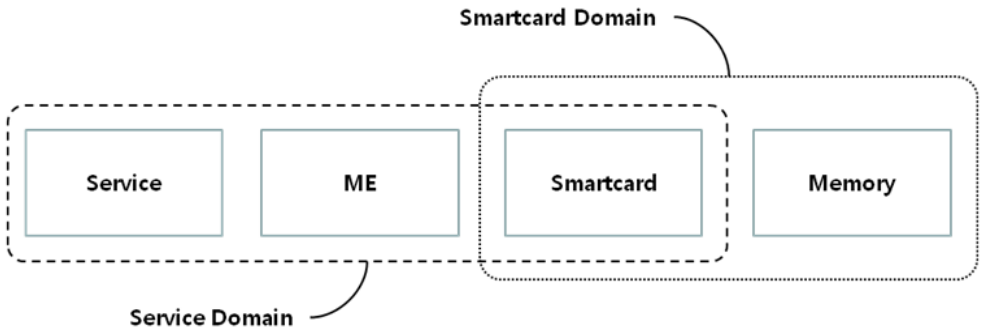

Figure 2. Classification of Security Models

The security model for service domain defined the roles and purpose of participants in the application environment from the security point of view and established the trusted relationship between participants. The security model for smartcard domain defined the security functions and roles between applet, smartcard (COS, platform, processor, EEPROM), and flash memory.

In this Section, we focus on the service-related security model in the service domain area. The smartcard domain area is handled in Section 4 interoperating with the high capacity USIM secure storage.

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. For the trusted relationship, we considered the protocol flow. 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 [Figure 3].

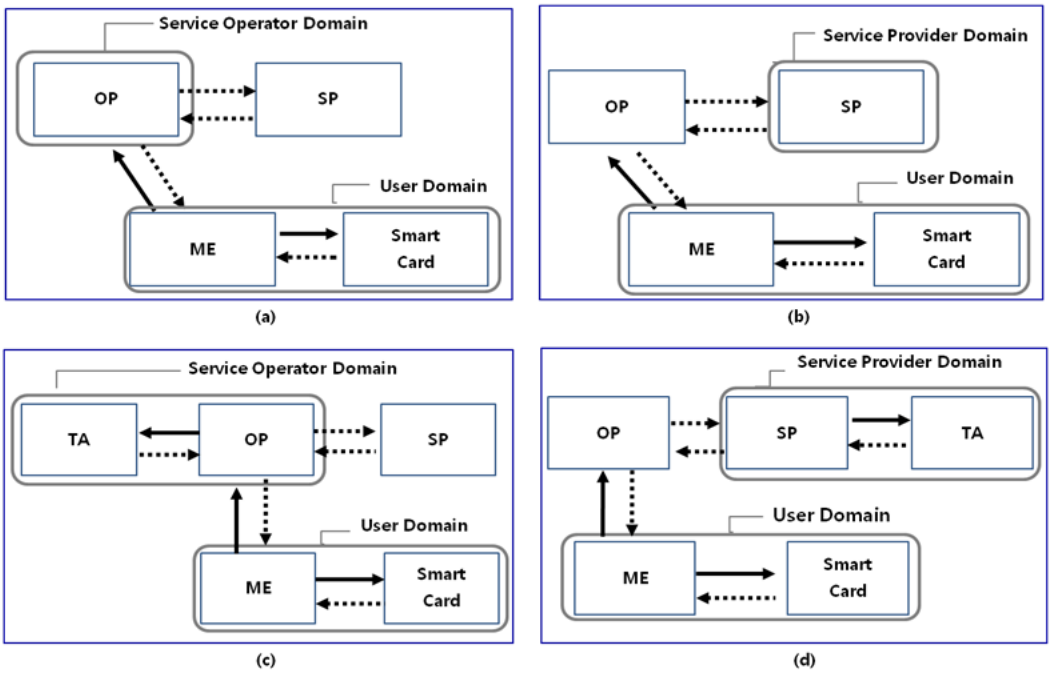

Figure 3. Trusted Relationship between Entities for Security Models (a: Basic Security Model, b: External Security Model, c: Asymmetric Security Model, d: Public Security Model)

While in the basic security model and asymmetric security model, the services are provided around an operator, the external security model and public security model provide services around a service provider. The related terms and symbols are as follows:

Table 2. 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.

Table 3 shows the characteristics for different security models.

Table 3. Comparison between Security Models

Security Model	Domain	Platform Technology	Protection Scope	Feature	Applied Field
Basic Security Model	Service Operator Domain	Symmetric key cryptography	- Confidentiality, authentication, and payment in the mobile zone - Service operator dedicated service protection	- Communication efficiency: Very efficient - Calculation efficiency: Very efficient - General use: Low (for closed services) - Security: High - Restriction: Key must be shared for subscription	- USIM - Point rewarding service - DRM
External Security Model	Service Provider Domain	Symmetric key cryptography	- Protection for non-network services - Nondisclosure and authentication for service-oriented confidential data	- Communication efficiency: Very efficient - Calculation efficiency: Very efficient - General use: Usual - Security: Usual - Restriction: Key must be shared for subscription	- e-money - Transportation card
Asymmetric Security Model	Service Operator Domain	PKI	- General purpose authentication in the operator domain - E2E cryptography in the operator domain	- Communication efficiency: Usual - Calculation efficiency: Low - General use: Usual - Security: High (non-repudiation is provided)	- OMA DRM 2.0 - CP authentication and cryptography
Public Security Model	Service Provider Domain	PKI	- General purpose authentication - E2E cryptography with the general wired server	- Communication efficiency: Low - Calculation efficiency: Low - General use: High - Security: High (non-repudiation is provided)	- Internet banking - Authentication and cryptography for the general wired server

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. Technically, the model is based on the secret key that is used in the symmetric key algorithm. Therefore, it is very efficient. Because the USIM card of a user stores its secret key after subscription, public key-based channel encryption and authentication are not additionally performed.

The external security model has the same features from the technical point of view. According to the issuer of the secret key, the model is classified into the basic security model and external security model. 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. Technically, for calculation of public key, huge amount of computation (1000 times more than the symmetric key algorithm) is required. For verification of the certificate, additional communication is required so it is less efficient.

Meanwhile, different from the basic and external security models that can provide security only when the key is shared, authentication and encryption are possible between different entities. Due to high usability and generality, the model is widely used despite low efficiency.

According to the trusted agency's location (asymmetric security model: service operator domain, public security model: service provider domain), the asymmetric and public security models are identified. Because the certificate that is used in the public security model is used for general purpose, hierarchical certificate issuance is made by multiple certificate authorities. Accordingly, the public security model costs much (for communication and computation) for verification of the certificate. Meanwhile, because in the asymmetric security model, the service operator hires the trusted agency, a unique certificate can be used for services. It is very efficient.

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. Secure Storage System for USIM-based Services

Abovementioned four different security models have their own characteristics and merits/demerits. Considering environmental factors, we have to choose an optimal security model for application.

4.1 Secure storage architecture

According to four security models in Section 3, basically the smartcard does not trust mobile equipment (ME). This is because any unprivileged terminal can access a specific data or service on the target smartcard by cheating. Accordingly, the smartcard must verify whether the connected terminal has privilege. At this time, a user authentication key is required. Actually PIN is used as the key. User enters the key on the terminal for authentication.

On the smartcard, MMSK and MSK are stored. MSK is the master key of the card issuer that is stored on the smartcard during card issuance or received later. MMSK is the unique master secret key of a smartcard and it is embedded when purchased so even the card issuer does not know this key. MMSK and MSK stored on a tamper-resistant smartcard cannot be accessed by any user, service provider or card issuer. (Only card issuer knows MSK.) A

smartcard performs encryption or decryption with two secret keys without disclosing them for providing encoded or decoded data.

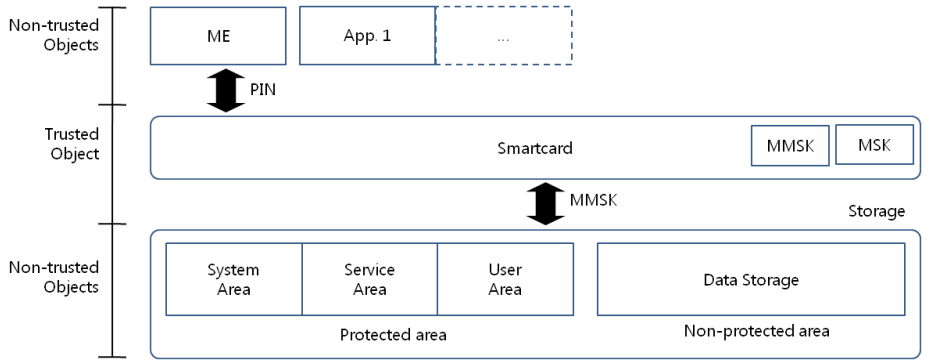

Figure 4. Secure Storage Architecture

Definitions for individual keys and notations are as follows:

Table 4. Terms and Keys

Term	Description	Remarks
EKEY(Data)	Secure encryption of data using the key	Encryption algorithm AES/128 bit
H(Data)	Hash value for the data calculated using the cryptographic hash function	The hash function SHA-1 is used.
MAC(KEY||Data)	Fixed length of value driven from the data by using the key	HMAC is used.
MSK	Only the card issuer (e.g. SKT) knows this master secret key. Users cannot know this.	Key length: 128 bit
MMSK	No one knows this unique master secret key of a smartcard.	Key length: 128 bit
SAK	System key	Key length: 128 bit
SK	Service key. Unique key for each service	Key length: 128 bit
SID	Service ID. Unique ID for each service Both card issuer and user cannot know this.	SID length: 4 bit
KU,i	Key for encryption of the user area	Key length: 128 bit

The protection area in storage can be accessed by the privilege subject only. For this purpose, each individual data is saved after being encrypted. For furthermore information about the key and encryption/decryption technique for each area, see the following descriptions.

4.2 Security for system area

The system area of high capacity USIM storage consists of the key storage area that stores all keys and the application area that stores various applications. As shown in Figure 5, the key storage area stores keys including the service key for service area. Various encrypted keys are also stored in this area. To encode each folder, a unique key of the folder is

generated. The key used for encryption is generated as the following through the master session key (MSK) and hash function SHA-1. (SAK = System Area Key).

$$SAK=HMAC(MSK||\text{“Key storage”}),\ SAK=HMAC(MSK||\text{“Application”})..\qquad (1)$$

Using the secure attention key (SAK) generated as shown above, the data is securely stored by encrypting each folder.

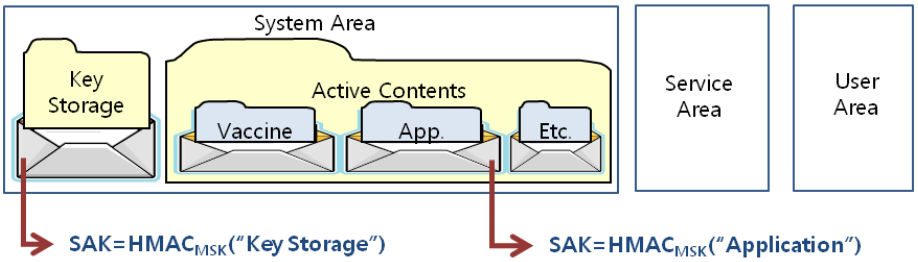

Figure 5. System Area Architecture

The following shows the encryption process for applications, which uses MSK and hash function (SHA-1 in this case) to generate SAK. The encryption with SAK allows storing application data securely [Figure 6]. Through this, only the actor that knows MSK can read or write the data in the system area.

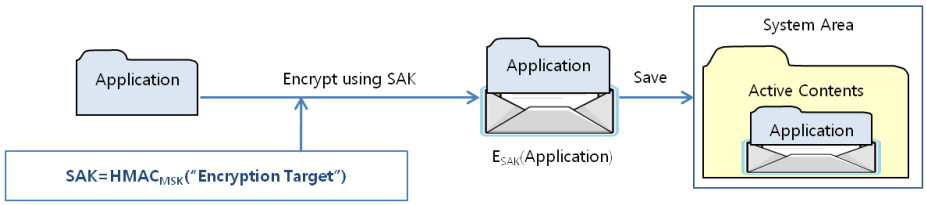

Figure 6. Encryption Protocol in System Area

The following describes the steps for the encryption protocol in the system area.

- Step 1: Fetches MSK to generate the encryption key for the folder in the system area of the smartcard.
- Step 2: The smartcard uses MSK to generate SAKs (=MSK||”Encryption Target”) for each encryption target.
- Step 3: The smartcard uses SAK to encrypt the folder keys or content data in the form of ESAK ("Encryption Target") for securely storing them.

4.3 Security for service area

The service area is a secure storage that can be used by any service or content provider. Generally, it is managed by the sub key in the system area. Even if the user has a valid PIN, he or she cannot access the service area. In addition, each individual service provider can have a unique allocation area defined by the service ID or the like. As shown in Figure 7, SID

is a unique ID granted to a service and SK is a unique secret key that corresponds to each service. The service key must not be disclosed to both card issuer and user.

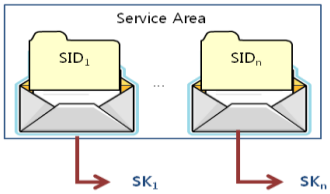

Figure 7. Service Area Architecture

In order to encrypt each service area and store the service key on the system area, the service or content provider must perform the service registration protocol [Figure 8]. The service registration protocol is run between the service provider and smartcard. While running the protocol, the service key must not be disclosed to the card issuer. For this purpose, the RSA encryption algorithm (asymmetric algorithm) is used. This commutative symmetry password meets the following conditions.

$$D_B(E_A(E_B(S\_Data)))=E_A(S\_Data) \quad (2)$$

- (S_Data: Required information including the service application and content)

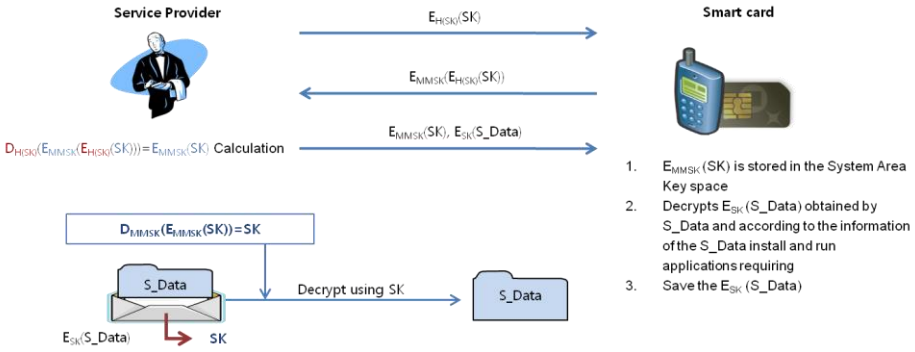

Figure 8. Service Key Registration Protocol

The following describes the steps for the service registration protocol.

- Step 1: The service provider generates the service key (SK) and calculates H(SK). Using H(SK), the service key is encrypted and the encrypted value is sent to the smartcard.
- Step 2: After encrypting $E_{H(SK)}(SK)$ ($E_{MMSK(EH(SK))}(SK)$) by using MMSK as a encryption key, the smartcard sends this value to the service provider again.
- Step 3: Using the commutative symmetry feature of the RSA encryption algorithm, the service provider decrypt $E_{MMSK}(E_{H(SK)}(SK))$ that corresponds to the encryption key (H(SK)) generated in Step 1 as a private key ($D_{H(SK)}(E_{MMSK}(E_{H(SK)}(SK)))=E_{MMSK}(SK)$). The service provider sends to the smartcard $E_{SK}(S\_Data)$ and $E_{MMSK}(SK)$ encrypted for the related (S_Data) that are required for use of services.

- Step 4: The smartcard stores $E_{MMSK}(SK)$ in the key space of the system area. Using its own MMSK, the smartcard decrypts $E_{MMSK}(SK)$ to generate SK. After getting S_Data by decrypting $E_{SK}(S\_Data)$ through SK, the required applications are installed and run depending on S_Data.

4.4 Security for user area

The user area can be accessed by the user only. The service provider and card issuer cannot access the area because the area is not controlled by them. Access to the user area is controlled through encryption. Because only the user must access the area, encryption is required using the user own key. The user stores in this area the privacy information including SMS, addresses, and personal information and sensitive non-disclosure information. The user can store the folders classified to the taste of user and encrypt them using different keys for each folder. The folder encryption is possible using a key with no classification. In case of encryption using different keys, even if a key is disclosed, other folders are not affected.

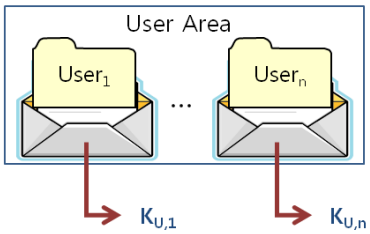

Figure 9. User Area Architecture

In order to encrypt individual folders stored in the user area, an encryption key is required. The encryption key is defined as the HMAC calculated with the user own PIN for index number and folder name. The user uses $HMAC_{PIN}(index\#||\ User_1)$ as the encryption key ($K_{U.1}$). The length of the encryption key is 128 bit and the key may vary depending on the folder name and index number. Each folder is encrypted using different encryption keys.

- Step 1: Creates the data for encryption key.
- Step 2: Using HMAC and user own PIN, different encryption keys are generated for each user area ($K_{U.1} = HMAC_{PIN}(index\#||\ User1)$)
- Step 3: Encrypts for each user area ($E_{KU.1}(User1)$)

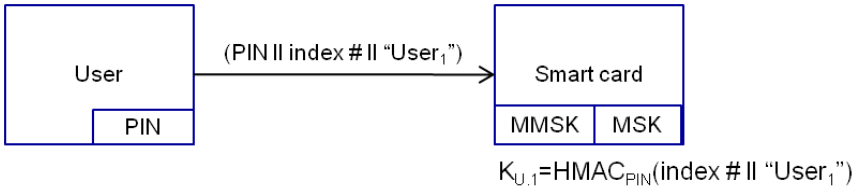

Figure 10. Generation of Encryption Key for User Area

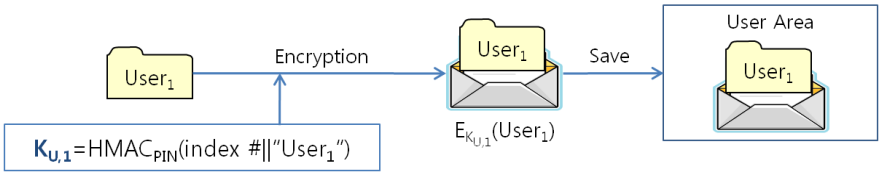

Figure 11. Access Control through User Area Encryption

5. Conclusion

In this paper, we suggested secure storage architectures for the high capacity USIM card, related technologies, and security models for services. Then we also suggested the secure storage control mechanisms for the suggested models.

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 requirements for the secure storage in high capacity USIM must be satisfied for security services such as USIM-based DRM. Accordingly, the requirements need to be applied for potential issues. 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] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 46, no. 1, **(2000)**, pp. 28-30.
[2] H. M. Sun, "An Efficient Remote User Authentication Scheme Using Smart Cards", IEEE Transactions on Consumer Electronics, vol. 46, no. 4, **(2000)**, pp. 958-961.
[3] H. Y. Chien, J. K. Jan and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card", Computers & Security, vol. 21, no. 4, **(2002)**, pp. 372-375.
[4] S. W. Lee, H. S. Kim and K. Y. Yoo, "Improved efficient remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 50, no. 2, **(2004)**, pp. 565-567.
[5] E. J. Yoon and K. Y. Yoo, "More Efficient and Secure Remote User Authentication Scheme using Smart Cards", Proc. of 11th International Conference on Parallel and Distributed System, vol. 2, **(2005)**, pp. 73–77.
[6] H. T. Liaw, J. F. Lin and W. C. Wu, "An efficient and complete remote user authentication scheme using smart cards", Mathematical and Computer Modeling, vol. 44, **(2006)**, pp. 223-228.
[7] C. Conrado, F. Kamperman, C. J. Schrijen and W. Jonker, "Privacy in an Identity-based DRM System", Proc. of the 14th IEEE Int. Workshop on Database and Expert Systems Applications, **(2003)**, pp. 389-395.
[8] H. M. Sun, C. F. Hung and C. M. Chen, "An Improved Digital Rights Management System Based on Smart Cards", Proc. of the International Conference on Digital EcoSystems and Technologies, Cairns, Australia, **(2007)**, pp. 308-313.
[9] M. Trampus, M. Ciglarit, M. PanEur and T. Vidmar, "Using Smart Cards as a Secure Storage for Digitally Signed Documents", EUROCON 2003, Computer as a Tool, The IEEE Region 8, vol. 2, **(2003)**, pp. 74-78.
[10] J. Hughes and C. Feist, "Architecture of the secure file system", Eighteenth IEEE Symposium on Mass Storage Systems, **(2001)**, pp. 277–290.
[11] P. Girard, "Which Security Policy for Multi application smart card", USENIX Workshop on Smartcard Technology, **(1999)**, pp. 21-28.