A Secure Mobile Digital ID Wallet using USIM of 3GPP

YunSeon Jung[1], SunHee Lim[1], Okyeon Yi[2], JongIn Lim[1], SeungHun Jin[3]
[1] Graduate School of Information Management and Security, Korea University
Tel: +82-2-3290-4251, Fax: +82-2-928-9109
E-mail: {jys2002, capsunny, jilim}@korea.ac.kr
[2] Department of Mathematics, Kookmin University
E-mail: oyyi@kookmin.ac.kr
[3] Electronics and Telecommunications Research Institute
E-mail: jinsh@etri.re.kr

***Abstract*? It is forecasted that the future 4G environments will see increase of IP-based services from the expansion of wireless internet and integration of wired and wireless networks, and the digital ID management technology in the wireless environments must be introduced to confront the illegal uses of personal data and other important communication structures. It therefore is imperative to study into the user ID management and the utilization of personal data for the 4G environment. The personal data management technology, using Digital ID Wallet, prevents the illegal access and possible damage that can occur from the distribution of personal information and further provides user-centered personal data and ID management technology. Moreover, it presents the new direction for Digital ID management that is suitable for wireless environment.**

I. INTRODUCTION

The expansion of wireless internet and the development of IP based services require the Digital ID management technology that can be used without the limits of time and place. A number of standardization committees are studying into identification management but they are not able to present a clear solution of Digital ID management that is appropriate for wireless environment[1,2]. In order for the future 4G environment and its related services to prosper, it is absolutely necessary to study and research the Digital ID management in wireless environment. Accordingly, it is required that the mobile terminal unit not only act as a simple communication equipment, but must takes on the role of medium to securely manage and control the personal data. The user ID and personal data are stored in USIM(Universal Subscriber Identity Module) instead of SP(Service Provider) and this can prevent the illegal use and distribution of personal information. Furthermore, the controllability of personal data utilization is put in the hands of the user and this makes it possible for ID management services to be centered on the user and provision of customized services. The use of authentication and access control mechanism GBA(Generic Bootstrapping Architecture), which is provided by 3GPP for application service, will enable the secure utilization of user's personal data for variety of services. This paper proposes Mobile Digital ID Wallet mechanism that provides the user ID management technology. In this technology, the user ID and personal data are stored at USIM, which acts as the authenticator in 3G network, and the technology is provided through the cooperation with USIM application. The proposed Mobile Digital ID Wallet will present a new direction for the management of Digital ID that is appropriate for the wireless environment.

II. NECESSITIES OF DIGITAL ID WALLET IN A MOBILE ENVIRONMENT [3]

In the existing Internet environment the users have to manage as the ID as the number of registered services. They have to undergo the inconvenience of input ID and Password every time for digital certification. They are faced with the risk of the identity theft because of the exposing their ID and Social Security Number. In the upcoming 4G wireless environment various services related to the financial and multimedia are expected to grow. This environment needs user-oriented mobile digital ID wallet mechanism so that users can use and control of their personal and certification information without the limits of time and place. The mobile digital ID wallet provides the ID-related services that perform sharing and managing personal and certification information.

III. THE 3GPP-LIBERTY INTERWORKING SYSTEM

3GPP TR 33.980 standard is defined as simple SSO(Single-Sign On) service of ID Federation in 3GPP-Liberty interworking system. SSO, using ID Federation, is a service where the user registers, modifies and manages all personal data of the subscribed services with one ID and the subscriber freely uses the information without additional authentication for a given period time after a single initial authentication. This chapter will describe authentication mechanism for 3GPP-Liberty interworking and SSO service mechanism.

A. System Architecture [4]

The proposed Digital ID Wallet in this paper is based on 3GPP TR 33.980 standard, which is the application of Liberty Alliance ID-FF/ID-WSF standard in the wireless environment. Figure 1 depicts the system structure for 3GPP-Liberty interworking, which is defined in 3GPP standard.

BSF(Bootstrapping Server Function) conveys the authenticating information between HSS(Home Subscriber Server) and UE(User Equipment) and relays key sharing between the

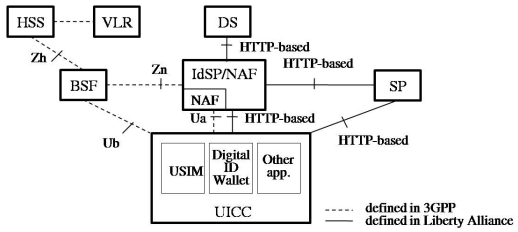

Figure 1. 3GPP-Liberty interworking architecture

SP and UE. NAF(Network Application Function) is the key center. IdSP(Identity Service Provider) can perform the role of NAF. IdSP provides the identity related services such as inquiring, authenticating, personal data managing and displaying, and verifies the authentication ticket. DS(Discovery Service) is one of the identification services, provided to search identity related information.

B. AKA(Authentication and Key Agreement) [5]

AKA procedure is defined in 3GPP 33.102 standard and depicts the execution of authentication and key agreement procedures between the user and network by using authentication vector AV. After the AKA procedure, USIM and HSS share the encryption key *CK* and integrity key *IK*.

C. GBA Bootstrapping [6]

GAA(Generic Authentication Architecture) is a security mechanism that provides the authentication and access control on mobile application services. In GAA there are SSC(Support for Subscriber Certificates) that communicates by using the certified authentication between the user and SP, and GBA that communicates by using the shared secret key. This paper bases on GBA. GBA is realized through Bootstrapping authentication procedure and Bootstrapping Usage procedure, where it is independent mechanism from SP.

a. Bootstrapping Authentication Procedure

Bootstrapping authentication procedure executes the interactive authentication between UE and HSS. Through this procedure BSF and UE share the secret key *Ks* that is generated by using *CK* and *IK* in AKA procedure.

b. Bootstrapping Usage Procedure

Bootstrapping Usage procedure is the key matching process where the session key between the user and the service requested by the user is matched. BSF generates and transmits *Ks_ext_IdSP* and *Ks_ext_SP* to each IdSP/NAF and SP. *B-TID* can be used as the user identity to secure anonymity of the linking user.

D. Single-Sign On based on GBA [6,7]

SSO authentication mechanism base on GBA uses artifact. UE and SP share the session key with AKA through Bootstrapping procedure. UE submits the artifact issued from IdSP to SP, and SP receives authentication of artifact by requesting assertion from IdSP. Assertion is authentication certificate that has user authentication and authorization information and artifact is reference pointer of source site that stores the assertion, which acts as the role of authentication ticket.

IV. THE COMMUNICATION BETWEEN UE AND UICC [8]

UICC and the mobile terminal unit communicate using APDU(Application Protocol Data Unit). UE retrieves the user data from USIM by using *READ RECORD* command and conveys the user data on Digital ID Wallet by using *UPDATE RECORD* command. *READ RECORD* command makes the response by inputting the user data into Data Field of Response APDU. *UPDATE RECORD* command makes delivery to Digital ID Wallet by inputting the user data into Data Field of Command APDU.

V. PROPOSED MOBILE DIGITAL ID WALLET MECHANISM USING USIM

The Mobile Digital ID Wallet, proposed in this paper, is similar to that of having a card kept in the wallet, which is a ticket that contain the generation of personal data specifically selected by the user, and authenticating and securely using the personal information for different services. The ticket can be either newly generated or issue the existing valid ticket with added necessary information. Digital ID Wallet, as depicted in figure 2, consists of the procedures of user registration, AKA and Bootstrapping of GBA, ticket generation and verification.

A. User Registration

When the user subscribes to 3G network, HSS generates *IMSI* to check the password key *K* and subscriber identity. After identifying the user by utilizing *IMSI*, *TMSI* and *LAI*, which is defined at 3GPP, the following procedures are executed.

1. HSS registers the user data at IdSP to verify the ticket.
2. The information of the corresponding user registers the address of the stored IdSP at DS.

B. AKA and Bootstrapping of GBA

AKA and Bootstrapping of GBA is the procedure where UE and HSS interactively authenticates and UE approves SP/IdSP and session key through BSF for the application service, and executes the procedure described in Ⅲ.A and Ⅲ.B. UE must be authenticated by HSS and IdSP and also the session key must satisfy the freshness prior to using the service. The shared session key *Ks_ext_SP* in this procedure is used in the next procedure, which is the encoding process for secure ticket transmission.

C. Ticket Generation and Verification

When the user registration and GBA Bootstrapping procedures are successfully completed, the following processes are executed.

3. UE sends Service Request message to SP.
4. SP, in order to obtain authentication information and additional information needed for the service, encrypts the corresponding IdSP information and the list of the other needed information with the session key *Ks_ext_SP* that is shared by Digital ID Wallet and sends Ticket Request message.
5. Digital ID Wallet application identifies the requested information list and checks for the existence of the authenti-

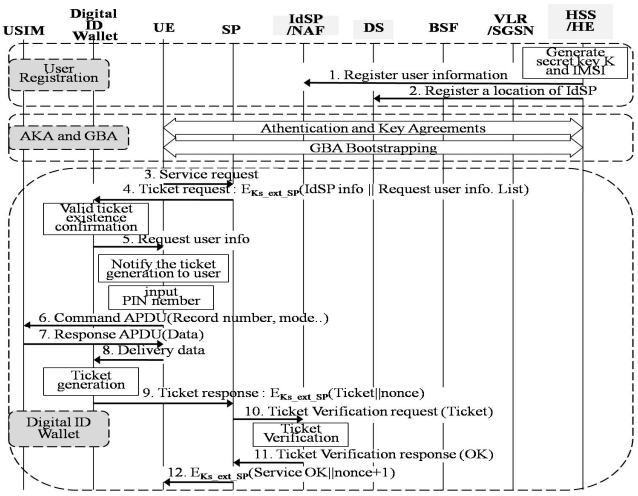

Figure 2. The Digital ID Wallet using User-issued Ticket

cation ticket that contains the requested information. If the ticket does not exist, then Digital ID Wallet will generate a new ticket. If a valid authentication ticket exists, then Digital ID Wallet can issue the ticket with only adding the needed information. Digital ID Wallet notifies the user of the ticket generation through UE and receives approval to use the personal information through input reception of PIN number.

6. UE notifies a request command for information to USIM using what is introduced in Ⅳ.

7. UE receives the needed information from USIM. using what is introduced in Ⅳ

8. UE relays the received information from USIM to Digital ID Wallet. Digital ID Wallet generates the ticket.

9. Ticket is encrypted with the session key *Ks_ext_SP* that is shared by Digital ID Wallet and sent to SP.

10. SP sends the ticket with Ticket Verification Request message to IdSP.

11. IdSP verifies the received ticket. If ticket is verified in success, then OK message is sent in Ticket Verification Response.

12. SP notifies UE to commence the service.

Table I compares the scenario of 3GPP-Liberty, introduced in Ⅲ.D, and Mobile Digital ID Wallet, proposed in this paper.

3GPP-Liberty proposed scenario, which is Federated identity management method, only provides the simple SSO. In this scenario, IdSP, which issues the artifact that basically is the counterpart of the authentication ticket and the stores the assertion that contains the actual authenticated information, acts as the main constituent in managing the user's personal information and this requires absolute trust of the user. Mobile Digital ID Wallet, on the other hand, proposes user-centered ID management technology in wireless environment. The focus of the user-centered ID management is that the user personally manages and controls the personal data. Of course the initial ID issuing requires registering the personal information into IdSP, however in the subsequent sessions the user personally decides the ID and personal information that are to be shared with SP for ticket generation. Furthermore, with having a single IdSP authentication, when the user requests for different SP service, IdSP searches DS and provides the ticket to the appropriate IdSP with the corresponding SP for authentication, which allows SSO.

Where 3GPP-Liberty scenario does not use USIM at all, the user's ID and the personal data are stored in USIM of Mobile Digital ID Wallet and this accordingly allows the management and control by the user Since the ticket, unlike the assertion, selects and generates the only needed information for any specific service, the problem of exposing unnecessarily excessive data to SP is prevented and insures necessary control of personal information. Therefore, illegal use and distribution of user information by a third party can be prevented. It can store personal information including the authentication data such as transfer approvals, financial and accounting; and if additional information is required even during the reception of a service, then any of the above information can be added to generate and submit a ticket, which means the possibility to provide customized services and to expand into variety of value-added activities. Accordingly, Mobile Digital ID Wallet makes it possible to insure the secure management and control of the personal information by the user, in addition to the functions of the basic authentication ticket-used SSO

VI. ANALYSIS

A. Efficiency

The upcoming 4G environment predicts integrated wire and wireless network and integrated heterogeneous network from the expansion of wireless internet. This will allow the user continuous break-free use of internet even through shifting from 3GPP network to non-3GPP network. This means that the user of Mobile Digital ID Wallet in 4G environment can move from one COT(Circle of Trust) to another COT and the existing IdSP will find the IdSP of the COT through DS in order to provide the ticket. And this smooth and natural shifting between the networks eliminates the users' uneasy feeling that their ID is somehow controlled at several different points. This enables the reception of real-time services such as multimedia under a continuous break-free condition.

B. Safeness

Mobile Digital ID Wallet is secure from eavesdropping, impersonation attacks, replay attacks, message forgery attacks

TABLE I. Compare the 3GPP-Liberty Scenario with the Mobile Digital ID Wallet

	3GPP-Liberty	Digital ID Wallet
ID management method	ID federated	user-centered
The subject of the ticket issue	IdSP	User
The subject of personal information management	IdSP	User
The store location of personal information	IdSP	USIM
The independence for IdSP	high	low
SSO	O	O
The Control of personal information	X	O

and redirection attacks as they are discussed in the following.

a. Eavesdropping and Information leakage

A passive adversary may eavesdrop the communication between UE and SP, but the message is first encrypted to the session key that UE and SP share through GBA Bootstrapping procedure and then sent. Therefore, the adversary does not know what are the requested information in SP or what information are contained in the ticket.

b. Impersonation attack

In this Impersonation attack, an active attack form, a malicious adversary impersonates as a justified SP and requests the user's authentication ticket or impersonates as a justified UE and provides a ticket. A malicious adversary would not however hold a justified session key *Ks_ext_SP* that has been generated through UE and GBA Bootstrapping procedure because this adversary did not participanted GBA Bootstrapping. Consequently, the adversary cannot send a justified ticket request message to UE or encrypted ticket to SP and thus impersonation attack is impossible.

c. Replay attack

In this Replay attack, an active attack form, the adversary acts as a justified UE, where a malicious adversary eavesdrops and stores the message that is being transmitted from UE to SP and re-transmits to SP at the next session. In order for the adversary to act as a justified UE to re-transmit the ticket to SP, the adversary must have the user's PIN number and this number must match with the number stored at USIM. But, the adversary is holding only the ticket and even if the adversary has the user's PIN number it will not match against the PIN number stored in the adversary's USIM; and when the adversary inputs the PIN number, it matches the number stored at USIM but does not match the ticket. Wrongfully inputting the PIN number to a specific number of times will terminate the access to USIM card, making it impossible to Replay attack.

d. Message forgery attack

USIM card is one of a smart card with innate characteristic of Tamper Resistance and thus an adversary cannot read the stored information off from USIM. For an adversary to attack SP with message forgery, it must hold the user's USIM card and has access to the user's PIN number and session key *Ks_ext_SP*. Furthermore, the adversary's forged ticket will not match the information against IdSP that is stored through IdSP ticket verification procedure, in result suspending a proper authentication. This is only possible by a proper user or HSS and makes it impossible for an adversary to conduct forgery attacks.

e. Redirection attack.

In Redirection attack, a malicious adversary snags the ticket being sent from UE to SP and responds service OK signal to UE, and redirects to a malicious SP. Service OK message encrypts into *Ks_ext_SP* with inclusion of nonce+1, which is an increase of value 1 compared to nonce sent with the user ticket, and therefore the Redirection attack can be detected when it contains the value that is different from nonce value selected by Digital ID Wallet.

f. Traceability

SP that has a record of providing a service to a user, although does not directly store the particulars of the user information, will log the record of what service has been provided to a particular identity. If the identity of a user can be traced, then an adversary may obtain sensitive and private information, such as preferences and inclinations of the user. Anonymity is possible by using the *B-TID* as the identity that BSF generates with *RAND* value and BSF tag in the GBA Bootstrapping procedure. *B-TID* is generated into new value at every execution of Bootstrapping procedure and therefore a malicious adversary cannot trace an anonymous user.

VII. CONCLUSIONS

This paper proposes, for the first time of its kind, a user-centered Digital ID management technology in the wireless environment. Mobile Digital ID Wallet utilized USIM card of 3GPP to provide ID management technology in wireless IP based service environment. Digital ID Wallet application is added to USIM and the user personally generates and submits the ticket by using the session key shared through GBA Bootstrapping. And this ultimately enables the user to manage and control personal ID and information. This has the advantages of simply following the direction of service changes, which demands the user-friendliness and customization, and the need to safely manage the personal identification without the limits of time and place.

Future foresees the need to design and develop further into Digital ID Wallet that can provide wider variety of services in more complicated integration of networks.

ACKNOWLEDGMENT

¡This work was supported by the IT R&D program of MIC/IITA. [IITA-2007-S-601-01, User Control Enhanced Digital Identity Wallet System]¡

¡This work was supported by the 2007 Research Fund of Kookmin University and the Kookmin Research Center UICRC in Korea¡

¡This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement)¡ (IITA-2008-(C1090-0801-0025))

REFERENCES

[1] WS-Security, http://msdn2.microsoft.com/enus/library/ms951273.aspx

[2] Liberty Alliance, Liberty ID-WSF Overview , 2007

[3] Dongho Song, ¡A Digital ID Purse Mechanism using USIM in a Mobile Environment ¡, Innovations 07, unpublished

[4] 3GPP TR 33.980: Liberty Alliance and 3GPP security interworking; ID-FF, ID-WSF and GAA, Release 7, 2007

[5] 3GPP TS 33.102: 3G Security; Security architecture, Release 7, 2006

[6] 3GPP TS 33.220: Generic Authentication Architecture(GAA); Generic bootstrapping architecture, Release 8, 2007

[7] Liberty Alliance, ID-WSF v2.0: Liberty ID-WSF Authentication, SSO, and Identity Mapping Service Specification, 2007

[8] 3GPP TS 31.102: Characteristics of the Universal Subscriber Identity Module(USIM) application, Release 7, 2007