Implementation for Federated Single Sign-on based on Network Identity

Kwihoon Kim*, Sengkyun Jo*, Hyunwoo Lee*, Won Ryu*

** Electrics and Telecommunications Research Institute*

161 Gajeong-Dong, Yuseong-Gu, Daejeon 305-700, Korea

Tel: +82-42-860-6746, Fax: +82-42-861-1342

E-mail: {kwihooi, skjo, hwlee, wlyu}@etri.re.kr

***Abstract*— This paper proposes a secure and fast one-pass authentication procedure bundling NACF and IMS authentications under enhanced security. Proposed scheme considerably reduces the complexity of authentication procedure compared to existing approaches. This paper mainly focuses on method authenticating federation Single Sign-on (SSO) about application service and IMS service based on network id in the Next Generation Networks (NGN) environment. Federation SSO is the one method of Single Sign-on which user can select the subscription of federation operator in real-time. For comprising this system, we need Service Control Function (SCF), Network Access Control Function (NACF), Web Application Service Control Function (WASCF) and NGN Terminal Function (NTF). Currently, certificate is used in internet banking. But, if real-time security monitoring tool is not operated, the exposure of certificate is very easy. For One Time Password (OTP) terminal case, it is lack with compatibility. If PC is detected by hacker, there is a problem. Through this paper, we propose the procedure to intercept originally the exposure of personal information in the internet. Therefore we suppose the procedure supporting Federation SSO authentication based on network id. That is, authentication system of reliable network operator can authenticate web application service (internet banking and so on).**

***Keywords*— NGN, NACF, SSO, Authentication, Federation**

I. INTRODUCTION

This paper is fully related with NGN. We deal with the method supporting Federation SSO authentication based on Network ID. This technique is SSO which authenticates web application service and IMS service such as internet banking based on reliable network authentication. This paper comprised with two cases. One is the Federation SSO and the IMS Federation SSO authentication using access network id.

Currently, the Next Generation Network (NGN) standards are developed by ITU-T to accommodate various wired/wireless access networks. Those standards aim to support several popular multimedia services including VoIP, IPTV, and instant messaging service. The NGN is divided into two logical planes: transport and service stratum. The transport stratum contains the functions for network attachment, resource management and data transport. A function in the transport stratum, called Network Attachment Control Function (NACF), manages authentication, registration, and initialization of the user equipment (UE) to access the NGN. The service stratum provides the functions for service control, application support, and service support to various multimedia applications. The NGN employs the IP Multimedia Subsystem (IMS) using the Session Initiation Protocol (SIP) for those multimedia service control signaling.

When a user registers IMS services, the authentications are required both for network access (by the NACF) and service accesses (by the IMS system). These two separated procedures incur considerable latency and message overhead to establish a service in NGN. Those individual procedures can be accelerated by integration of access and service authentication operations. Some bundled approaches have been proposed to tie up the NACF and IMS authentication procedures [1], [2]. However, they suffer from a security problem on their signaling. In this paper, we propose a new bundled authentication scheme for mobile users in the NGN, which employ the secure signaling for authentication between the UE and IMS system.

II. RELATED WORKS

Previous technique is such as following. In the Liberty Alliance, there is Federation SSO authentication among applications. For using this technique, if user authenticates the application service which has taken a role of Identity Provider, user doesn't have to authenticate another application service. But, this technique has the weak point that because Identity Provider is web application the danger of hacking is large. Therefore we need to propose more secure method through using Identity Provider with reliable network equipment such as NACF or IMS

OTP (password generator for one time) and certificate are frequently used through application authentication technique based on web application. Certificate is the representative user authentication system in the banking business area. If user has saved this in PC or hasn't installed security program, there are

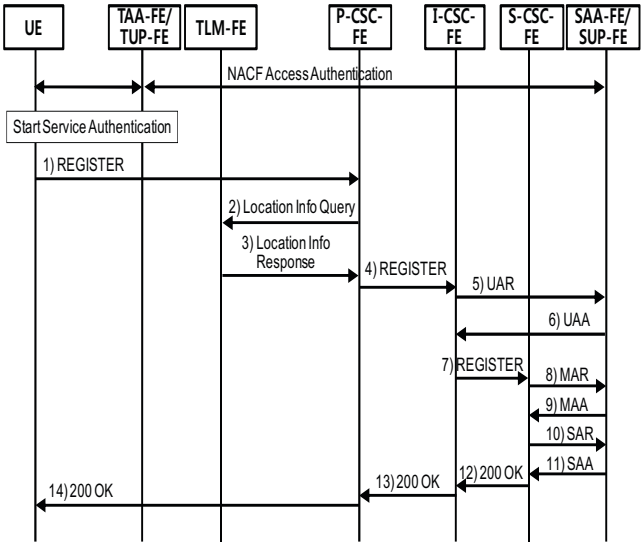

Figure 2. One-Pass Line-based NBA Procedure

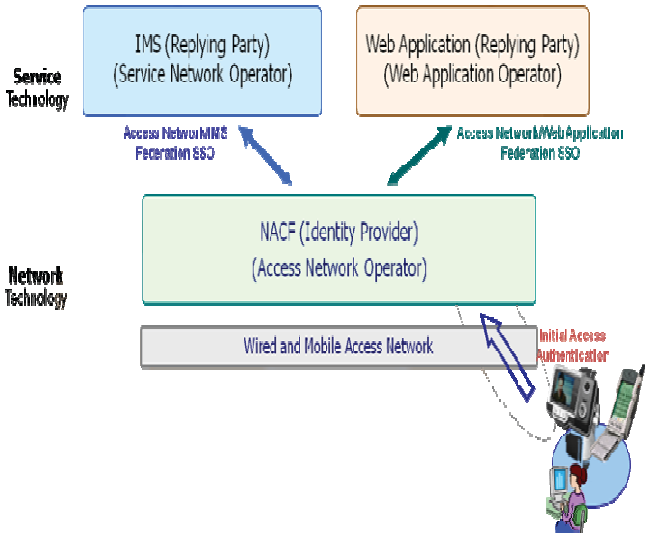

Figure 1. The network architecture for proposed federated SSO authentication based on Network ID

the problem of exposed password. Also, even though user installed security program, the problem of captured certificate occurs without acting real-time monitoring. OTP shares preliminarily the key values made by cryptograph and uses one time password every time. But, the problem of device compatibility and hacking PC itself exists.

Currently, for Next Generation Networks (NGN) in ITU-T (International Telecommunication Union - Telecommunication Standardization Sector) and TISPAN (The Telecoms & Internet converged Services & Protocols for Advanced Networks), when NACF L3 level authentication is completed, IMS L5 level authentication procedure will be omitted after checking bundle authentication subscription. And then, the information for bundle authentication subscription is provided by business operator. That is, after user request the operator about bundle authentication subscription, operator should change the information of subscriber. But when the access network operator has various service network operators, user must request each service network operator about bundle authentication subscription. Also, in case user requests service network authentication, if user doesn't subscribe bundle authentication, federation request procedure is needed.

In the 3GPP network, two-pass handshaking is required to complete service authentication in the IMS system [3]. Recently, the NACF bundled authentication (NBA) scheme in the NGN has been proposed to extend the NACF authentication procedure to the Service Control Function (SCF) layer [1]. Figure 1 shows the procedure of the NBA approach. When a UE requests a NGN attachment, the NACF authenticates a UE and allocates its IP address. Then the NACF stores the UE's layer-2 and layer-3 identifiers in its own profile. When the UE registers with the IMS service, the Proxy Call Session Control Functional Entity (P-CSC-FE) sends a query to the NACF to obtain the UE's location information. Subsequently, the P-CSC-FE sends a message containing the UE's location information to the Serving CSC-FE (S-CSC-FE). Then the S-CSC-FE compares the UE's location information with one obtained from the Service User Profile Functional Entity (SUP-FE). On successful verification, the user is successfully authenticated at the SCF layer. While four handshake steps (for two passes) are required for service authentication in the 3GPP network, only 2 handshake steps (for one pass) are needed in the bundled authentication procedure in Figure 1 (REGISTER / 200 Ok).

The aforementioned bundled authentication scheme has some drawbacks. First, it assumes that the NACF (actually, a TLM-FE) is connected to only a single P-CSC-FE. However, in the practical circumstance, several Transport Location Management Functional Entities (TLM-FEs) are connected to a single P-CSC-FE. This makes the P-CSC-FE difficult to determine which TLM-FE manages a specific UE's location information. The second one is the existing scheme identifies a user based on the information of fixed communication line. Since a mobile UE does not have the fixed line information, the additional access identifiers have to be added to the UE's profile [4], [5]. Finally, the existing schemes suffer from security weakness since it only compares the UE's location information without any security operations. A malicious user can be easily authenticated by spoofing the other user's IP address or line identifier.

In this paper, we propose the SSO authentication based on reliable network authentication instead of internet application authentication. Furthermore we suggest not the method operator set but the method user select.

III. PROPOSED SCHEME

This paper proposes to solve above noticed problem. Therefore in case user subscribes access network and concurrently various application services, Single Sign-on of federation method must be provided in NGN.

Here, we propose a secure single sign-on scheme of access

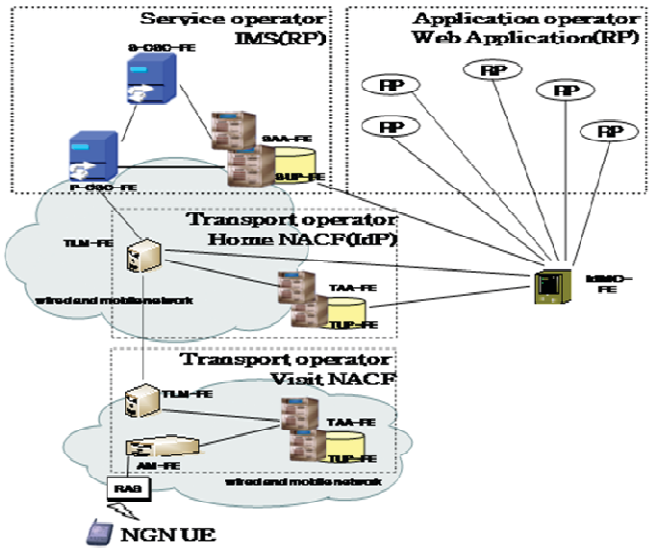

Figure 3. The network architecture for proposed federated SSO authentication based on Network ID

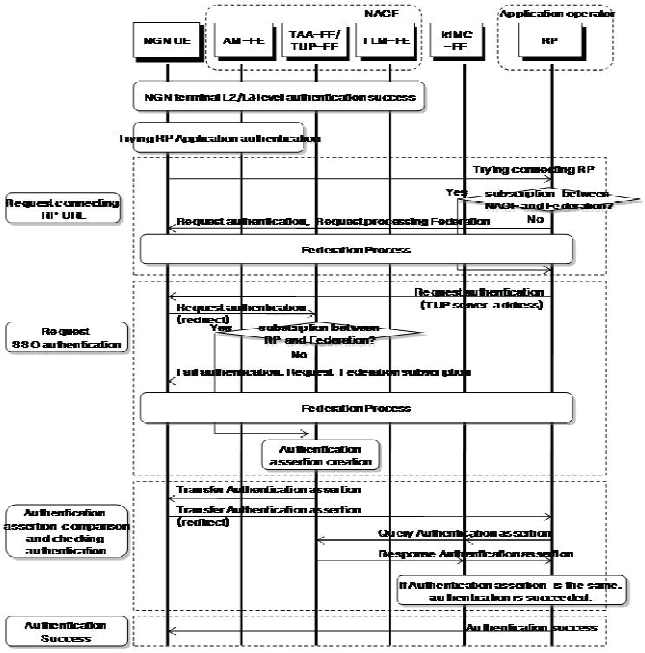

Figure 4. The procedure for proposed federated SSO authentication based on Network ID

and service authentications in NGN. Our scheme addresses the problems of the existing approaches by enhancing the security of authentication signaling. The main idea of the proposed scheme is to introduce the Authentication and Key Agreement (AKA) vector in 3GPP, which includes an Integrity Key (IK), a Cipher Key (CK), and a credential for authentication.

Access network operator provides the unified access authentication through the NACF irrespective of various wired and wireless network. NGN User Equipment (UE) can authenticate initially access network through unified wired and wireless access network.

Service network operator provides the IMS service authentication for NGN UE using SIP REGISTER. IMS authentication uses the method of MD5-Digest and MD5-AKA. We need to reduce IMS authentication procedure to simply this procedure through the NACF authentication information.

Web application operators provide authentication method based on ID and password for NGN UE. For proposed system, we can use network authentication for Identity Provider (IdP). Network authentication is operated by NACF TAA-FE. That is, when IdP authenticates initial access network, all Replying Party (RP) is omitted on Federation. At this time, authentication algorithm between IdP and UE is provided irrespectively.

Following figures 2, 3, 4 show the concept, architecture and procedure about proposed scheme.

IV. CONCLUSIONS

In the NGN, this paper proposed the federated authentication for Web Application service and IMS service authentication based on network ID. Though previous research considered authentication between Web application services, this paper provide SSO authentication between NACF and web application service through using Identity Provider with NACF. Therefore this scheme is more reliable than previous scheme.

Also, unified authentication for access network and IMS service network is possible through operator. However proposed scheme supports user to select promptly SSO authentication. Through this method when one access network related with various service network operators, it is useful. In single service network case, a user can subscribe easily SSO authentication. For the future, this technique can use the unified billing system based on NGN.

For further Study, the performance evaluation in various aspects will be determined.

ACKNOWLEDGMENT

This work was supported by the IT R&D program of KCC/MKE/KEIT. [2009-S-018-01, Development of Open-IPTV Platform Technologies for IPTV Convergence Service and Content Sharing]

REFERENCES

[1] ETSI, “TISPAN Security Architecture,” *TS 187 003*, Jan. 2006.

[2] ITU-T, “Functional Requirements and Architecture of the NGN of Release 1,” *Rec. Y.2012*, Sept. 2006.

[3] 3GPP, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security, Security Architecture,” *TS 33.102*, June 2003.

[4] ITU-T, “Requirements and protocol at the interface between service control entity and the transport location management physical entity,” *Rec. Q.3221*, Oct. 2008.

[5] R. Melen, M. Pignolo, and M. Sioli, “A Multimodal Authentication System for Authorizing the Access to NGN Services,” *Proc. International Conference on Networking and Services*, July 2006.

...