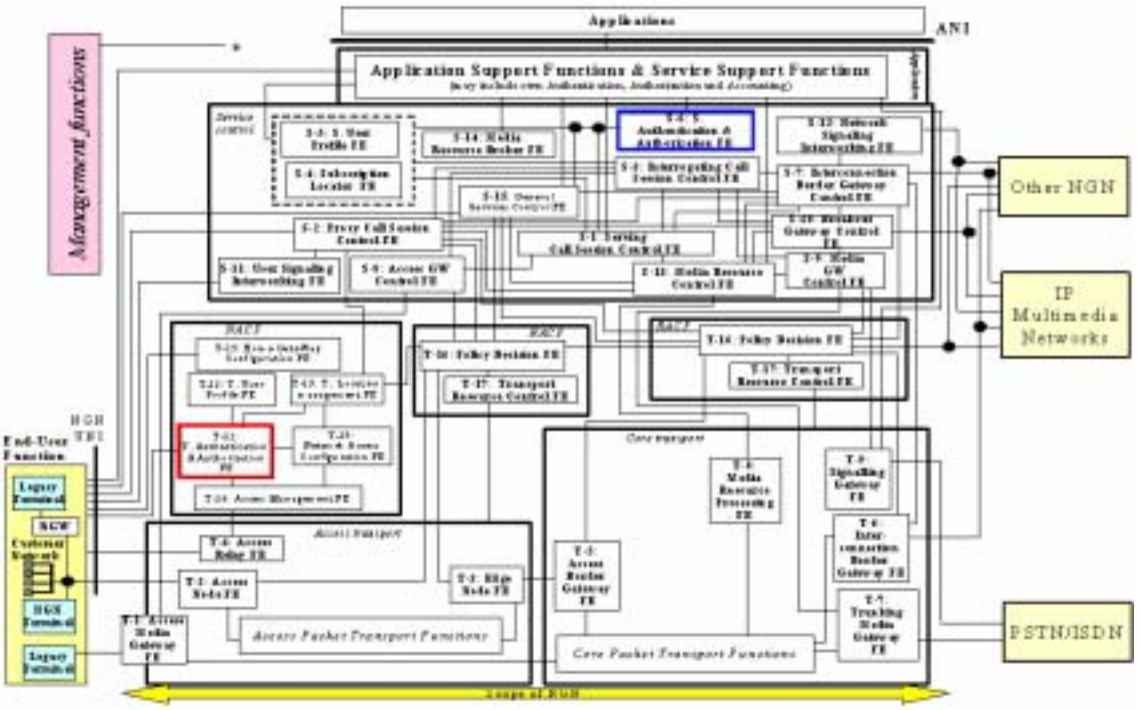
[전송통신] NGN 망에서의 식별 및 인증(Identification and Authentication)

NGN 네트워크에서 인증정보

사용자가 NGN 서비스를 이용하기 위해서는 인증자(예, P-CSCF, NAP)로부터 가입자 및 단말에 대한 식별 및 인증을 받아야 한다. 이러한 과정은 인증자(Authenticator)와 CPE(Customer Premises Equipment) 간에 인증정보(Credential)를 교환함으로써 이루어진다. NGN에서 인증정보는 X.509 인증서와 공유 비밀키 2가지로 분류된다. X.509 인증서와 공유 비밀키는 NGN 네트워크 요소들 간 또는 CPE와 인증자 간에 안전한 전달 채널을 형성하는데 사용된다. 또한 공유 비밀키는 인증자가 CPE의 초기 요청 메시지(SIP INVITE 또는 REGISTER 메시지 인증 과정)를 검증하는데 사용될 수도 있다. 공유 비밀키는 인증 서버 AAA의 역할을 수행하는 SAA(Service Authentication Authorization)/TAA(Transport Authentication Authorization)-FEs와 사용자 역할을 수행하는 subscriber 또는 end-user가 각각 공유한다.

NGN 보안 구조에서는 인증정보를 device 인증정보, subscriber 인증정보, end-user 인증정보로 분류한다. Device 인증정보(예, 단말 시리얼 번호)는 단말 제조업체에서 생성하는 정보로 NGN 네트워크에서 단말을 식별하고 인증하는 정보이다. Subscriber 인증정보는 NGN 서비스에 가입한 후, 서비스를 이용할 수 있는 인증정보를 SIM 카드 등에 저장된 것을 말한다. Subscriber는 사람이 아닌 서비스 관련 인증정보를 SIM 카드에 저장하고, 이 SIM 카드를 사용하여 서비스를 이용할 수 있는 인증정보 자체를 말한다. End-user 인증정보는 특정 사용자를 식별 및 인증하는 정보이다. 또는, end-user는 subscriber와 관련된 서비스를 이용하는 사람이라고 정의할 수 있다. Subscriber와 end-user는 하나의 같은 객체로 볼 수도 있고, 하나의 subscriber에 여러 end-user로 구성될 수 있다. 예를 들어 어떤 서비스에 가입된 정보가 담겨 있는 SIM 카드를 사용하여 여러 사람들이 각각 다른 단말기에 장착하여 사용하는 경우를 말한다.



<그림 1> NGN FRA 구조에서 TAA/SAA-FE

SAA/TAA-FE는 device, subscriber, end-user에 대한 각각의 인증정보들을 모두 저장 및 관리한다. 이동성이 지원되는 단말의 경우, 단말 또는 사용자의 아이디를 사용하여 외부 네트워크의 인증 서버가 홈 네트워크 인증서버인 SAA/TAA-FE에 저장되어 있는 인증정보를 요청하여 단말을 인증하고 서비스를 제공할 수 있다. 표 1은 SAA/TAA-FE에 저장되어 있는 인증정보의 한 예이다.

<표 1> SAA/TAA-FE 에 저장된 인증정보 예

For a subscriber certificate assigned to the John Doe family: Subscriber Account : Doe-family From headers : sip:*Doe@NGN .ngn.com Identity string : sip:Doe@NGN .ngn.com Type of credentials : subscriber End-User ID required : no	For a pre-shared key assigned to the John Doe family: Key name : JohnDoe Key : dfe56131d1958046689d83306477ecc From headers : sip:*Doe@NGN .ngn.com Identity string : sip:Doe@NGN .ngn.com Type of credentials : subscriber End-User ID required : no

Subscriber 및 End-user의 식별 및 인증

시그널링 프로토콜인 SIP INVITE 메시지의 From 헤더에 subscriber에 대한 아이디가 포함된다. 그러나 이 아이디는 공격자에 의해 손쉽게 위조가 가능하므로 정당한 subscriber에 대한 식별 및 인증을 수행할 수 없다. Subscriber 식별 및 인증 기법으로는 SIP 요청 메시지의 소스 아이피 매핑, TLS/IPSec 보안 채널 사용, challenge/response 방법과 같이 세가지로 분류된다. IP 매핑 방법은 가장 간단한 방법이고, TLS/IPSec 보안 채널을 통한 SIP 메

시지 전달 방법은 X.509 인증서 기반의 방식이다. Challenge/response 방식은 SIP 요청 메시지에 대해서 프락시 서버인 P-CSCF가 임의의 랜덤값으로 SIP 요청자에게 응답하고, SIP 요청자가 사용자 아이디와 패스워드를 사용하여 적절한 인증정보를 생성할 수 있는지 확인을 통해 식별 및 인증을 수행하는 방식이다. 이 세가지 방식 중 시그널링을 위한 인증 방법으로 사용되는 것은 TLS/IPSec 보안 채널과 challenge/response 방식이다.

인증자와 인증서버 간 인터페이스

NGN 네트워크에서는 사용자 및 단말에 대한 인증정보가 없는 인증자(Authenticator)가 모든 인증정보를 저장 및 관리하는 인증서버(SAA/TAA-FE)에게 인증정보를 요청하여 사용자를 인증한다. 그리고 대량의 인증 요청 메시지가 하나의 SAA/TAA-FE에 집중되는 부하를 분산시키기 위해서 여러 인증자들 사이에 SAA/TAA-FE가 분산되어 배치될 수도 있다. 이러한 구조에서 인증자와 SAA/TAA-FE 간 통신 프로토콜이 요구된다. RADIUS와 DIAMETER 프로토콜이 이러한 목적을 위하여 사용된다. 인증자는 RADIUS/DIAMETER 클라이언트가 되고, SAA/TAA-FE는 RADIUS/DIAMETER의 서버 역할을 수행한다.

정수환 (숭실대학교 정보통신전자공학부 교수, souhwanj@ssu.ac.kr)