(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0144739
(43) 공개일자 2022년10월27일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *H04L 65/40* (2022.01)
H04W 12/10 (2021.01) *H04W 4/60* (2018.01)
(52) CPC특허분류
H04L 63/0892 (2013.01)
H04L 63/083 (2013.01)
(21) 출원번호 10-2021-0059580
(22) 출원일자 2021년05월07일
심사청구일자 없음
(30) 우선권주장
1020210051321 2021년04월20일 대한민국(KR)

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
손중제
경기도 수원시 영통구 삼성로 129(매탄동)
이덕기
경기도 수원시 영통구 삼성로 129(매탄동)
(74) 대리인
윤앤리특허법인(유한)

전체 청구항 수 : 총 1 항

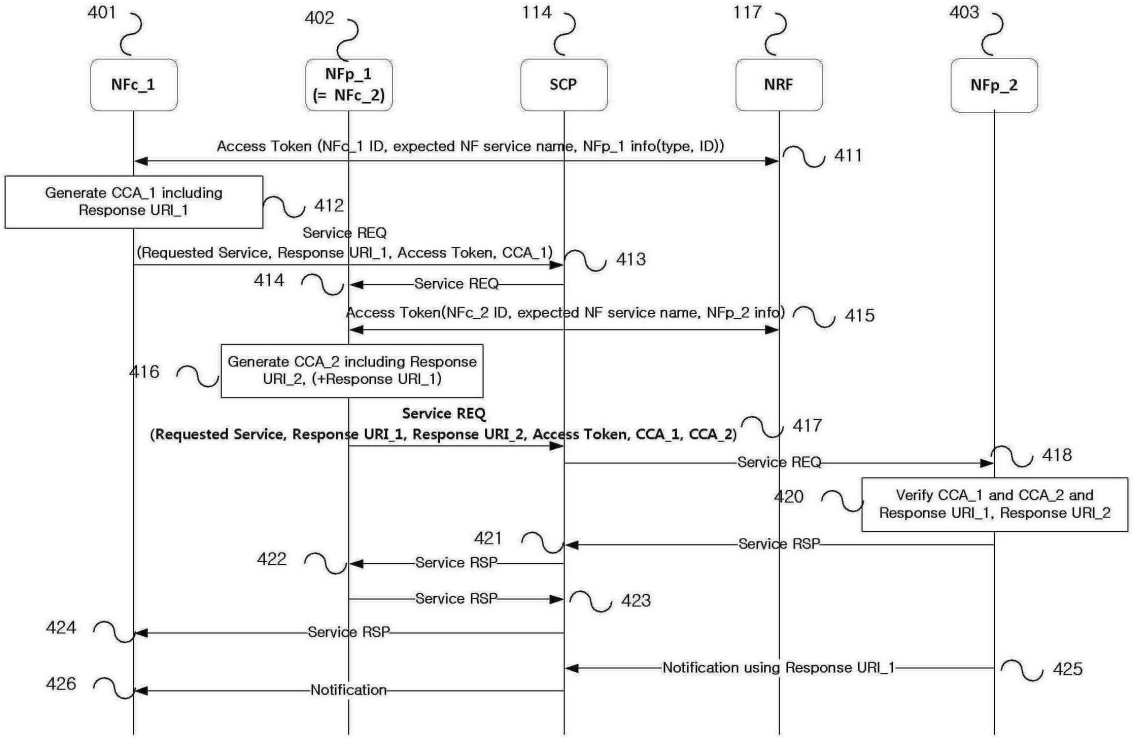
(54) 발명의 명칭 **이동통신 시스템의 네트워크 장치 간 인증 방법 및 장치**

(57) 요 약

본 개시는 4G 시스템 이후 보다 높은 데이터 전송률을 지원하기 위한 5G 통신 시스템을 IoT 기술과 융합하는 통신 기법 및 그 시스템에 관한 것이다. 본 개시는 5G 통신 기술 및 IoT 관련 기술을 기반으로 지능형 서비스 (예를 들어, 스마트 홈, 스마트 빌딩, 스마트 시티, 스마트 카 혹은 커넥티드 카, 헬스 케어, 디지털 교육, 소매업,

(뒷면에 계속)

대 표 도



보안 및 안전 관련 서비스 등)에 적용될 수 있다.

본 개시의 일 실시예에 따른 방법은, 이동통신 시스템의 제2네트워크 기능(network function, NF)에서 제3NF로부터의 서비스 인증 방법으로, 제1NF로부터 상기 제3NF로부터의 서비스를 요청하는 서비스 요청 메시지를 수신하는 단계, 상기 제1서비스 요청 메시지는 서비스를 제공하기 위한 UE의 식별 정보, 이벤트 지시자(event id) 및 NF 저장소 기능(NRF)로부터 획득된 제1토큰을 포함하고; 상기 제1서비스 요청 메시지를 인증하는 단계; 상기 제1NF의 요청을 수행하기 위해 상기 NRF로부터 제2토큰을 획득하는 단계; 상기 제1서비스 요청 메시지에 포함된 정보를 포함하고, 상기 제2토큰을 포함하여 상기 제3NF로 서비스 요청 메시지를 전송하는 단계; 및 상기 제3NF로부터 서비스 응답 메시지를 수신할 시 이를 상기 제1NF로 제공하는 단계;를 포함할 수 있다.

(52) CPC특허분류

H04L 67/51 (2022.05)

H04W 12/10 (2021.01)

H04W 4/60 (2018.02)

명 세 서

청구범위

청구항 1

이동통신 시스템의 제2네트워크 기능(network function, NF)에서 제3NF로부터의 서비스 인증 방법에 있어서,

제1NF로부터 상기 제3NF로부터의 서비스를 요청하는 서비스 요청 메시지를 수신하는 단계, 상기 제1서비스 요청 메시지는 서비스를 제공하기 위한 UE의 식별 정보, 이벤트 지시자(event id) 및 NF 저장소 기능(NRF)로부터 획득된 제1토큰을 포함하고;

상기 제1서비스 요청 메시지를 인증하는 단계;

상기 제1NF의 요청을 수행하기 위해 상기 NRF로부터 제2토큰을 획득하는 단계;

상기 제1서비스 요청 메시지에 포함된 정보를 포함하고, 상기 제2토큰을 포함하여 상기 제3NF로 서비스 요청 메시지를 전송하는 단계; 및

상기 제3NF로부터 서비스 응답 메시지를 수신할 시 이를 상기 제1NF로 제공하는 단계;를 포함하는, 이동통신 시스템의 제2NF에서 제1NF로 제3NF로부터의 서비스 인증 방법.

발명의 설명

기 술 분 야

[0001] 본 개시는 이동통신 시스템 내 네트워크 장치 간 인증 방법 및 장치에 관한 것으로, 특히 네트워크 장치 간의 연결에서 네트워크 장치의 인증 및 권한 관리를 위한 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 4G 통신 시스템 상용화 이후 증가 추세에 있는 무선 데이터 트래픽 수요를 충족시키기 위해, 개선된 5G 통신 시스템 또는 pre-5G 통신 시스템을 개발하기 위한 노력이 이루어지고 있다. 이러한 이유로, 5G 통신 시스템 또는 pre-5G 통신 시스템은 4G 네트워크 이후 (Beyond 4G Network) 통신 시스템 또는 LTE 시스템 이후 (Post LTE) 이후의 시스템이라 불리어지고 있다. 높은 데이터 전송률을 달성하기 위해, 5G 통신 시스템은 초고주파(mmWave) 대역 (예를 들어, 60기가(60GHz) 대역과 같은)에서의 구현이 고려되고 있다. 초고주파 대역에서의 전파의 경로 손실 완화 및 전파의 전달 거리를 증가시키기 위해, 5G 통신 시스템에서는 빔포밍(beamforming), 거대 배열 다중 입출력(massive MIMO), 전차원 다중입출력(Full Dimensional MIMO: FD-MIMO), 어레이 안테나(array antenna), 아날로그 빔형성(analog beam-forming), 및 대규모 안테나 (large scale antenna) 기술들이 논의되고 있다. 또한 시스템의 네트워크 개선을 위해, 5G 통신 시스템에서는 진화된 소형 셀, 개선된 소형 셀 (advanced small cell), 클라우드 무선 액세스 네트워크 (cloud radio access network: cloud RAN), 초고밀도 네트워크 (ultra-dense network), 기기 간 통신 (Device to Device communication: D2D), 무선 백홀 (wireless backhaul), 이동 네트워크 (moving network), 협력 통신 (cooperative communication), CoMP (Coordinated Multi-Points), 및 수신 간섭제거 (interference cancellation) 등의 기술 개발이 이루어지고 있다. 이 밖에도, 5G 시스템에서는 진보된 코딩 변조(Advanced Coding Modulation: ACM) 방식인 FQAM (Hybrid FSK and QAM Modulation) 및 SWSC (Sliding Window Superposition Coding)과, 진보된 접속 기술인 FBMC(Filter Bank Multi Carrier), NOMA(non orthogonal multiple access), 및SCMA(sparse code multiple access) 등이 개발되고 있다.

[0003] 한편, 인터넷은 인간이 정보를 생성하고 소비하는 인간 중심의 연결 망에서, 사물 등 분산된 구성 요소들 간에 정보를 주고 받아 처리하는 IoT(Internet of Things, 사물인터넷) 망으로 진화하고 있다. 클라우드 서버 등과의 연결을 통한 빅데이터(Big data) 처리 기술 등이 IoT 기술에 결합된 IoE (Internet of Everything) 기술도 대두되고 있다. IoT를 구현하기 위해서, 센싱 기술, 유무선 통신 및 네트워크 인프라, 서비스 인터페이스 기술, 및 보안 기술과 같은 기술 요소 들이 요구되어, 최근에는 사물간의 연결을 위한 센서 네트워크(sensor

network), 사물 통신(Machine to Machine, M2M), MTC(Machine Type Communication)등의 기술이 연구되고 있다. IoT 환경에서는 연결된 사물들에서 생성된 데이터를 수집, 분석하여 인간의 삶에 새로운 가치를 창출하는 지능형 IT(Internet Technology) 서비스가 제공될 수 있다. IoT는 기존의 IT(information technology)기술과 다양한 산업 간의 융합 및 복합을 통하여 스마트홈, 스마트 빌딩, 스마트 시티, 스마트 카 혹은 커넥티드 카, 스마트 그리드, 헬스 케어, 스마트 가전, 첨단의료서비스 등의 분야에 응용될 수 있다.

[0004] 이에, 5G 통신 시스템을 IoT 망에 적용하기 위한 다양한 시도들이 이루어지고 있다. 예를 들어, 센서 네트워크(sensor network), 사물 통신(Machine to Machine, M2M), MTC(Machine Type Communication)등의 기술이 5G 통신 기술인 빔 포밍, MIMO, 및 어레이 안테나 등의 기법에 의해 구현되고 있는 것이다. 앞서 설명한 빅데이터 처리 기술로써 클라우드 무선 액세스 네트워크(cloud RAN)가 적용되는 것도 5G 기술과 IoT 기술 융합의 일 예라고 할 수 있을 것이다.

발명의 내용

해결하려는 과제

[0005] 이동통신 시스템 단말의 네트워크 접속 및 데이터 수신 관리를 위한 이동통신 시스템 내 네트워크 장치 간 연결에서 단말의 데이터를 통보 받는 네트워크 장치의 인증 및 권한 관리를 위한 방법에 관한 것이다.

과제의 해결 수단

[0006] 본 개시의 일 실시예에 따른 방법은, 이동통신 시스템의 제2네트워크 기능(network function, NF)에서 제3NF로부터의 서비스 인증 방법으로, 제1NF로부터 상기 제3NF로부터의 서비스를 요청하는 서비스 요청 메시지를 수신하는 단계, 상기 제1서비스 요청 메시지는 서비스를 제공하기 위한 UE의 식별 정보, 이벤트 지시자(event id) 및 NF 저장소 기능(NRF)로부터 획득된 제1토큰을 포함하고; 상기 제1서비스 요청 메시지를 인증하는 단계; 상기 제1NF의 요청을 수행하기 위해 상기 NRF로부터 제2토큰을 획득하는 단계; 상기 제1서비스 요청 메시지에 포함된 정보를 포함하고, 상기 제2토큰을 포함하여 상기 제3NF로 서비스 요청 메시지를 전송하는 단계; 및 상기 제3NF로부터 서비스 응답 메시지를 수신할 시 이를 상기 제1NF로 제공하는 단계;를 포함할 수 있다.

발명의 효과

[0007] 본 개시에 따르면, 네트워크 장치 간에 구독 및 통지 모델을 통하여 서비스를 요청하고, 이에 대한 인증 및 허가를 수행할 수 있다. 특히 service consumer가 직접 service provider에게 요청할 수도 있고, service provider가 제2의 service provider에게 service consumer로 서비스를 요청할 수도 있다.

도면의 간단한 설명

[0008] 도 1은 본 개시의 실시 예에 따른 5G 이동통신 시스템의 구조이다.

도 2는 본 개시의 실시 예에 따른 네트워크 장치의 시스템 등록 절차에 대한 예시도이다.

도 3은 본 개시의 실시 예에 따른 네트워크 장치의 접근 권한 허가 및 토큰 취득 절차에 대한 예시도이다.

도 4는 본 개시의 실시 예에 따른 네트워크 장치 인증서를 활용한 네트워크 장치 간 SUBSCRIBE-NOTIFICATION 모델의 서비스 요청 및 회신의 인증 및 권한 허가 절차에 대한 예시도이다.

도 5는 본 개시의 실시 예에 따른 네트워크 장치의 시스템 등록 정보를 활용한 네트워크 장치 간 SUBSCRIBE-NOTIFICATION 모델의 서비스 요청 및 회신의 인증 및 권한 허가 절차에 대한 예시도이다.

도 6는 본 개시의 실시 예에 따른 네트워크 장치의 인증서를 활용한 네트워크 장치 간 SUBSCRIBE-NOTIFICATION 모델의 서비스 요청 및 회신의 인증 및 권한 허가 절차에 대한 예시도이다.

도 7는 본 개시의 실시 예에 따른 네트워크 장치의 토큰 발행 정보를 활용하여, 네트워크 장치 간 SUBSCRIBE-NOTIFICATION 모델의 서비스 요청 및 회신의 인증 및 권한 허가 절차에 대한 예시도이다.

도 8은 본 개시의 다양한 실시예에 따른 네트워크 기능(NF) 장치의 블록 구성도이다.

도 9는 본 개시의 실시 예에 네트워크 장치 집합 정보를 활용한 네트워크 장치 간 REQUEST-RESPONSE 모델의 서비스 요청 및 회신의 인증 및 권한 허가 절차에 대한 예시도이다.

도 10은 본 개시의 실시 예에 따른 네트워크 장치 집합 내의 네트워크 장치 선택을 활용한 네트워크 장치 간 REQUEST-RESPONSE 모델의 서비스 요청 및 회신의 인증 및 권한 허가 절차에 대한 예시도이다.

발명을 실시하기 위한 구체적인 내용

[0009] 이하, 첨부된 도면들을 참조하여 다양한 실시 예들을 상세히 설명한다. 이때, 첨부된 도면들에서 동일한 구성요소는 가능한 동일한 부호로 나타내고 있음에 유의해야 한다. 또한 이하에 첨부된 본 발명의 도면은 본 발명의 이해를 돕기 위해 제공되는 것으로, 본 발명의 도면에 예시된 형태 또는 배치 등에 본 발명이 제한되지 않음에 유의해야 한다. 또한 본 발명의 요지를 흐리게 할 수 있는 공지 기능 및 구성에 대한 상세한 설명은 생략할 것이다. 하기의 설명에서는 본 발명의 다양한 실시 예들에 따른 동작을 이해하는데 필요한 부분만이 설명되며, 그 이외 부분의 설명은 본 발명의 요지를 흩트리지 않도록 생략될 것이라는 것을 유의하여야 한다.

[0010] 도 1은 본 발명의 실시 예에 따른 5G 이동통신 시스템의 구조도이다.

[0011] 도 1을 참조하기에 앞서 5G 이동통신 시스템의 코어 네트워크에서 각 기능들을 수행하는 단위는 네트워크 기능(network function, NF)으로 정의될 수 있다. 이러한 네트워크 기능은 특정한 서버 또는 네트워크 장치에 구현될 수 있다. 네트워크 기능이 특정한 서버 또는 네트워크 장치에 구현되는 경우 하나의 특정한 서버(또는 네트워크 장치)에 둘 이상의 네트워크 기능을 탑재할 수 있다. 탑재된다는 의미는 네트워크 기능을 수행하는 장치로 동작함을 의미할 수 있다. 네트워크 기능이 서버에 탑재되는 경우 동일한 기능을 수행하는 서로 다른 둘 이상의 네트워크 기능이 탑재될 수 있다. 서로 다른 둘 이상의 네트워크 기능은 동일한 동작을 제어하는 네트워크 기능일 수도 있고, 서로 다른 네트워크 기능일 수도 있다.

[0012] 하나의 서버에 동일한 네트워크 기능이 둘 이상 포함되는 경우를 예를 들면, 사용자 장치(user equipment, UE)로 사용자 데이터를 제공하는 사용자 평면 네트워크 기능(user plane function, UPF)가 하나의 서버 내에 둘 이상 존재할 수 있다. 다른 예로, 하나의 서버 내에 서로 다른 네트워크 기능들이 탑재되는 경우를 예를 들면, UPF와 세션 관리 기능(session management function, SMF)가 하나의 서버 내에 탑재될 수도 있다.

[0013] 또 다른 예로, 하나의 네트워크 기능이 서로 다른 둘 이상의 서버(또는 네트워크 장치)로 구현될 수도 있다. 예컨대, 하나의 UPF가 둘 이상의 서버를 통해 구현될 수도 있다.

[0014] 이상에서 설명한 바와 같이 본 명세서에서 설명되는 5G 코어(core) 네트워크의 네트워크 기능들은 네트워크 내에서 특정한 동작을 하는 하나의 엔티티를 지칭하는 용어로, 단순한 기능이 아닌 서버 또는 네트워크 장치로 구현될 수 있음에 유의해야 한다.

[0015] 도 1을 참조하면, UE(10)는 적어도 5G 네트워크에 접속 가능한 단말이 될 수 있다. UE(10)는 그 외에 다른 무선 접속 방식 예를 들어, 4G 네트워크 및/또는 WiFi 네트워크 등의 다양한 네트워크와 접속할 수도 있다. 또한 UE(10)는 다양한 형태를 가질 수 있다. 예컨대, IoT 기능만을 제공하는 단말로 구현되거나, 또는 스마트, 태블릿 컴퓨터와 같은 형태일 수도 있고, 스마트 워치 또는 스마트 글래스와 같은 웨어러블 형태의 기기로 구현될 수도 있다. 본 개시에서 UE(10)의 구현 형태에는 특별한 제약을 두지 않는다.

[0016] 무선 접속 노드(radio access node, (R)AN)(20)는 UE(10)와 5G 무선 접속 방식으로 air 상의 신호 또는 데이터의 송수신을 수행하는 네트워크 노드가 될 수 있다. 또한 (R)AN(20)은 4G 무선 액세스 기술의 진화된 버전인 진화된 E-UTRA(evolved E-UTRA)와 새로운 무선 액세스 기술(new radio, NR)(예를 들어, gNB)을 모두 지원하는 새로운 무선 액세스 네트워크를 총칭할 수 있다.

[0017] 다음으로 5G 코어 네트워크를 구성하는 NF들에 대하여 살펴보기로 한다. 도 1에 예시된 NF들은 사용자 평면 기능(user plane function, UPF)(110), 인증 서버 기능(authentication server function, AUSF)(111), 액세스 및 이동성 관리 기능(access and mobility management function, AMF)(112), 세션 관리 기능(session management function, SMF)(113), 서비스 통신 프록시(Service Communication Proxy, SCP)(114), 네트워크 슬라이스 선택 기능(Network Slice Selection Function, NSSF)(115), 네트워크 노출 기능(network exposure function, NEF)(116), NF 저장소 기능(NF repository function, NRF)(117), 정책 및 제어 긴으(policy and control function, PCF)(118), 통합된 데이터 관리(unified data management, UDM)(119) 및 어플리케이션 기능(application function, AF)(120)를 포함할 수 있다.

[0018] UPF(110)는 DN(180)으로부터 수신한 하향링크 PDU를 (R)AN(20)을 경유하여 UE(10)에게 전달하며, (R)AN(20)을 경유하여 UE(10)로부터 수신한 상향링크 PDU를 DN(180)으로 전달할 수 있다. 구체적으로, UPF(110)는 인트라(intra)/인터(inter) RAT 이동성을 위한 앵커 포인트, 데이터 네트워크(Data Network)로의 상호연결

(interconnect)의 외부 PDU 세션 포인트, 패킷 라우팅 및 포워딩, 패킷 검사(inspection) 및 정책 규칙 시행의 사용자 평면 부분, 합법적 감청(lawful intercept), 트래픽 사용량 보고, 데이터 네트워크로의 트래픽 플로우의 라우팅을 지원하기 위한 상향링크 분류자(classifier), 멀티-홈(multi-homed) PDU 세션을 지원하기 위한 브랜치 포인트(branching point), 사용자 평면을 위한 QoS 핸들링(handling)(예를 들어 패킷 필터링, 게이팅(gating), 상향링크/하향링크 레이트 시행), 상향링크 트래픽 검증 (서비스 데이터 플로우(service data flow, SDF)와 QoS 플로우 간 SDF 매핑), 상향링크 및 하향링크 내 전달 레벨(transport level) 패킷 마킹, 하향링크 패킷 버퍼링 및 하향링크 데이터 통지 트리거링 기능 등을 지원할 수 있다.

[0019] AUSF(111)는 UE(10)의 인증을 위한 데이터를 처리하고 저장할 수 있다. 또한, AUSF(111)는 3GPP 접속 네트워크와 비-3GPP(non-3GPP) 접속 네트워크에서 UE(10)의 인증을 수행할 수 있다.

[0020] AMF(112)는 UE 단위의 접속 및 이동성 관리를 위한 기능을 제공할 수 있으며, 하나의 UE 당 기본적으로 하나의 AMF에 연결될 수 있다. 구체적으로, AMF(112)는 3GPP 액세스 네트워크들 간의 이동성을 위한 CN 노드 간 시그널링, 무선 액세스 네트워크(radio access network, RAN) CP 인터페이스(즉, N2 인터페이스)의 종단(termination), NAS 시그널링의 종단(N1), NAS 시그널링 보안(NAS 암호화(ciphering) 및 무결성 보호(integrity protection)), AS 보안 제어, 등록 관리(등록 영역(registration area) 관리), 연결 관리, 아이들 모드 UE 접근성(reachability)(페이징 재전송의 제어 및 수행 포함), 이동성 관리 제어(가입 및 정책), 인트라-시스템 이동성 및 인터-시스템 이동성 지원, 네트워크 슬라이싱(network slicing)의 지원, SMF 선택, 합법적 감청(lawful intercept)(AMF 이벤트 및 LI 시스템으로의 인터페이스에 대한), UE와 SMF 간의 세션 관리(session management, SM) 메시지의 전달 제공, SM 메시지 라우팅을 위한 트랜스패런트 프록시(transparent proxy), 액세스 인증(access authentication), 로밍 권한 체크를 포함한 액세스 허가(access authorization), UE와 단문 메시지 서비스 기능(Short Message Service Function, SMSF) 간의 SMS 메시지의 전달 제공, 보안 앵커 기능(security anchor function, SAF) 및/또는 보안 컨텍스트 관리(security context management, SCM) 등의 기능을 지원할 수 있다. 이러한 AMF(112)의 일부 기능(들) 또는 전체의 기능들은 하나의 AMF로 동작하는 단일 AMF 인스턴스(instance) 내에서 지원될 수 있다. 또한 AMF(112)는 UE(10)의 보안 관련 기능을 담당하는 보안 앵커 기능(Security Anchor Function, SEAF)을 포함할 수 있다.

[0021] SMF(113)는 세션 관리 기능을 제공하며, UE(10)가 다수 개의 세션을 가지는 경우 각 세션 별로 서로 다른 SMF에 의해 관리될 수 있다. 구체적으로, SMF(113)는 세션 관리(예를 들어, UPF와 AN 노드 간의 터널(tunnel) 유지를 포함하여 세션 확립, 수정 및 해지), UE IP 주소 할당 및 관리(선택적으로 인증 포함), UP 기능의 선택 및 제어, UPF에서 트래픽을 적절한 목적지로 라우팅하기 위한 트래픽 스티어링(traffic steering) 설정, 정책 제어 기능(policy control functions)를 향한 인터페이스의 종단, 정책 및 서비스 품질(quality of service, QoS)의 제어 부분 시행, 합법적 감청(lawful intercept)(SM 이벤트 및 LI 시스템으로의 인터페이스에 대한), NAS 메시지의 SM 부분의 종단, 하향링크 데이터 통지(downlink data notification), AN 특정 SM 정보의 개시자(AMF를 경유하여 N2를 통해 AN에게 전달), 세션의 SSC 모드 결정, 로밍 기능 등의 기능을 지원할 수 있다. 앞에서 설명한 바와 같이 SMF(130)의 일부 기능(들) 또는 전체의 기능들은 하나의 SMF로 동작하는 단일 SMF 인스턴스(instance) 내에서 지원될 수 있다.

[0022] SCP(114)는 특정한 서로 다른 NF들 SCP(114)를 통해 간접 통신을 제공할 수 있다. 또한 SCP(114)는 보안 통신 예를 들어 NF 서비스 생산자(producer) API에 액세스하기 위한 NF 서비스 소비자(Consumer)의 권한 부여를 수행할 수 있고, 부하 분산, 모니터링, 과부하 제어 등을 수행할 수 있다. 즉, SCP(114)는 특정한 서로 다른 둘 이상의 NF들 간의 간접적인 통신 경로를 제공할 수 있다.

[0023] NSSF(115)는 UE(10)를 서비스하는 네트워크 슬라이스 인스턴스 세트 선택, 허용된 NSSAI 결정 및 필요한 경우 가입된 S-NSSAI에 대한 매핑, 구성된 NSSAI 결정 및 필요한 경우 가입된 S-NSSAI에 대한 매핑, UE(10)를 서비스하는데 사용될 AMF 세트를 결정하거나, 구성에 기초하여, 가능하면 NRF(117)를 쿼리함으로써 후보 AMF (들)의 목록을 결정할 수 있다.

[0024] NEF(116)는 네트워크 기능 능력(NF capability) 및 이벤트(event)를 외부 네트워크에 노출할 수 있다. 또한 NEF(116)는 통합된 데이터 저장소(Unified Data Repository, UDR)에 대한 표준화된 인터페이스(Nudr)를 사용하여 정보를 구조화 된 데이터로 저장 및 검색할 수 있다.

[0025] NRF(117)는 서비스 검색 기능을 지원한다. NF 인스턴스 또는 SCP(114)에서 NF 검색 요청을 수신하고 검색된 NF 인스턴스(검색 대상)의 정보를 NF 인스턴스 또는 SCP(114)로 제공한다. 또한 NRF(117)는 P-CSCF 디스커버리를 지원하고, 사용 가능한 NF 인스턴스 및 지원되는 서비스의 NF 프로필을 유지한다. 또한 NRF(117)는 신규 등록/

업데이트/등록 취소된 NF 인스턴스에 대해 NF 서비스와 함께 가입한 NF 서비스 소비자 또는 SCP(114)에게 알린다.

[0026] PCF(140)는 어플리케이션 서버로부터 패킷 흐름에 대한 정보를 수신하여, 이동성 관리, 세션 관리 등의 정책을 결정하는 기능을 제공할 수 있다. 구체적으로, PCF(140)는 네트워크 동작을 통제하기 위한 단일화된 정책 프레임워크 지원, 제어평면 기능(들)(예를 들어, AMF, SMF 등)이 정책 규칙을 시행할 수 있도록 정책 규칙 제공, 사용자 데이터 저장소(user data repository, UDR) 내 정책 결정을 위해 관련된 가입 정보에 액세스하기 위한 프론트 엔드(front end) 구현 등의 기능을 지원할 수 있다.

[0027] UDM(170)은 사용자의 가입 데이터, 정책 데이터 등을 저장할 수 있다. UDM(170)은 2개의 부분, 즉 어플리케이션 프론트 엔드(front end, FE)(미도시) 및 사용자 데이터 저장소(user data repository, UDR)(미도시)를 포함할 수 있다.

[0028] AF(150)는 서비스 제공(예를 들어, 트래픽 라우팅 상에서 어플리케이션 영향, 네트워크 능력 노출(network capability exposure)에 대한 접근, 정책 제어를 위한 정책 프레임워크와의 상호동작 등의 기능을 지원)을 위해 3GPP 코어 네트워크와 상호 동작할 수 있다.

[0029] 어플리케이션 기능(application function, AF)(120)은 서비스를 제공하기 위해 3GPP 코어 네트워크와 상호작용한다. 예컨대, 어플리케이션의 트래픽 라우팅에 관한 동작, NEF(116)에 접속(access), 정책 제어를 위한 정책 프레임 워크와의 상호 작용을 수행할 수 있다.

[0030] DN(130)은 예를 들어, 운영자 서비스, 인터넷 접속 또는 서드파티(3rd party) 서비스 등을 의미할 수 있다. DN(130)은 UPF(110)로 하향링크 프로토콜 데이터 유닛(protocol data unit, PDU)을 전송하거나, UE(10)로부터 전송된 PDU를 UPF(110)를 통해 수신할 수 있다.

[0031] 이상에서 설명한 도 1에 예시된 5G 코어 네트워크를 통해 UE(10)는 5G 네트워크 접속 및 데이터 송수신 등의 서비스를 제공받을 수 있다. 또한 5G 코어 네트워크는 UE(10)를 관리하기 위하여 상기 NF들간에 통신을 수행 할 수 있다. 이때, 상기 NF들은 NF 소비자(Consumer)와 NF 제공자(Producer)로서 동작을 하여 상호 간에 통신을 수행할 수 있다. NF Producer는 서버로서 NF Consumer들이 접속하여 NF Producer의 서비스를 받을 수 있도록 한다. NF Consumer는 NF Producer에 접속하여 NF Producer가 제공해주는 서비스를 사용한다. NF Producer와 NF Consumer는 NF Producer가 제공해주는 서비스를 사용하여 UE(10) 또는 네트워크 관련 제어나 관리를 위해서 필요한 동작을 수행할 수 있다.

[0032] NF Producer는 NF Consumer의 서비스 요청에 대한 응답으로 서비스를 제공해 줄 수 있다. 또한, NF Producer는 필요한 조건을 만족하는 경우, 데이터를 제공해 주는 통지 서비스(Notification)를 제공할 수 있다. 이때, NF Producer는 통지 서비스에 가입(Subscription)한 NF Consumer가 서비스 가입 시 등록한 정보에 기반하여 통지 서비스를 제공할 수 있다.

[0033] 본 개시의 실시 예에 따라서 NF Consumer와 NF Producer는 직접 통신을 할 수도 있고, 중간에 SCP(114)를 통해서 통신할 수도 있다. NF Consumer는 NF Producer에 대한 Service Request를 SCP(114)로 전송하고, SCP(114)는 수신한 NF Consumer의 Service Request를 요청 받은 대로 NF Producer에게 전송할 수 있다. NF와 NF 사이의 통신과, NF와 NRF 간의 통신은 모두 SCP(114)를 통해서 전송될 수 있다. 이때, NF Producer는 NF Consumer와 직접 통신을 수행하지 않으므로 NF Consumer가 Service Request 메시지에 포함하여(또는 함께) 제공하는 클라이언트 인증서(Client Credentials Assertion, CCA)를 통해서 NF Consumer를 인증할 수 있다.

[0034] 도 2는 본 개시의 실시 예에 따른 네트워크 장치에서 시스템 등록 절차를 설명하기 위한 예시도이다.

[0035] 도 2를 참조하면, 네트워크 기능(NF)(201)은 도 1에서 설명한 바와 같이 하나의 장치 또는 서버로 구현될 수 있다. 또한 NF(201)는 도 1에서 설명한 도 5G 코어 네트워크 내에 존재하는 NF들 중 어느 하나이거나 또는 NEF(116)를 통해 접속하는 AF(120)을 포함할 수 있다.

[0036] 그러면 도 2를 참조하여, NF(210)가 NRF(117)에 등록하기 위한 절차에 대하여 살펴보기로 한다. NF(201)는 최초 동작을 시작할 때(또는 활성화될 때), 221단계와 같이 네트워크 기능 프로파일(NF Profile)을 NRF(117)에 등록하기 위한 NF 등록 요청(NF Register Request) 메시지를 NRF(117)에 전송할 수 있다.

[0037] NF의 NF Profile은 다음과 같은 정보들 중 일부 또는 전부를 포함할 수 있다.

[0038] - 네트워크 기능 타입(NF Type): AMF(112), SMF(113) 등의 NF와 같이 자신의 종류를 지칭하는 타입 정보를 포함

할 수 있다.

[0039] - 네트워크 기능 인스턴스 지시자(NF Instance ID): 네트워크 기능 인스턴스를 지칭하는 지시자를 포함할 수 있다.

[0040] - NF의 IP 주소 또는 정규화된 도메인 이름(Fully Qualified Domain Name, FQDN)

[0041] - 지원되는 NF 서비스들의 이름 등의 정보

[0042] - NF가 속한 PLMN 정보

[0043] - NF가 관리하는 UE 또는 가입자 정보의 지시자 범위 또는 지시자 정보

[0044] 위의 정보들 중에서 네트워크 기능 인스턴스는 특정한 하나의 NF가 인스턴스(Instance) 형태로 구현될 수 있는 경우에 해당한다. 예컨대, AMF(112), SMF(113), UPF(110)와 같이 5G 코어 네트워크를 구성하는 NF들은 동일한 동작을 수행하는 둘 이상의 인스턴스들로 구성될 수 있다. 각 인스턴스들 특정한 도 1에서 설명한 동일한 기능을 수행할 수 있다. 예컨대, 서로 다른 두 개의 UPF(110)가 UPF 인스턴스들로 구성되고, 두 개의 UPF 인스턴스들 모두 동일한 UE로 사용자 평면 데이터를 제공할 수 있다. 이런 경우 각각의 UPF 인스턴스들은 서로 다른 사용자 데이터를 제공할 수 있다. 가령, 특정한 하나의 UPF 인스턴스는 다운로드 데이터 서비스를 제공하는 UPF가 될 수 있고, 다른 하나의 UPF 인스턴스는 데이터의 업로드를 제공하는 UPF가 될 수 있다. 또 다른 예로, 특정한 하나의 UPF 인스턴스는 영화의 스트리밍 서비스를 제공하고, 다른 하나의 UPF 인스턴스는 채팅 서비스를 제공할 수도 있다. 또한 위에서는 인스턴스 형태를 설명하였으나, 서로 다른 둘 이상의 UPF들이 하나의 UE로 서로 다른 서비스를 제공하는 경우에도 동일하게 적용될 수 있다. 또 다른 예로, UPF가 제공할 수 있는 데이터의 총 양에 기반하여 둘 이상의 UPF 또는 UPF 인스턴스들을 구현할 수도 있다.

[0045] 다시 도 2를 참조하면, NF(201)는 211단계에서 NRF(117)에 등록하는 NF Profile에 NF가 다른 NF에서 서비스를 제공받을 때 데이터를 수신할 수 있는 URI 주소 정보(Response URI)를 추가 할 수 있다. 또한 NF(201)가 다른 NF에 서비스를 제공해주는 NF Producer로 동작하는 경우, 해당 NF Producer의 서비스를 제공 받는 NF Consumer로 동작할 수 있는 NF type 이나 NF Instance ID 등을 NF profile에 추가할 수 있다.

[0046] NRF(117)는 212단계에서 NF(201)로부터 수신된 NF Profile 등록에 대한 요청 메시지를 수신한 경우, 해당 NF(201)의 NF Profile을 저장한 후, 213단계에서 NF(201)에게 NF 등록 응답(NF Register response) 메시지를 NF Register Request에 대한 응답으로 생성하여 회신할 수 있다.

[0047] 도 3은 본 개시의 실시 예에 따른 NF Consumer가 NF Producer의 서비스를 받고자 할 때, 해당 NF Producer의 서비스를 받을 수 있는지 NRF에게 접근 허가 및 토큰을 취득하는 절차를 예시한 도면이다.

[0048] 도 3을 참조하기에 앞서, NF 서비스 소비자(NF service Consumer) 또는 NF 소비자(NF Consumer)는 동일한 의미이며, 이하의 설명에서 동일한 NF로 설명한다. 따라서 NF 서비스 소비자 또는 NF 소비자가 혼용되더라도 동일한 의미로 이해되어야 할 것이다. 또한 NF 서비스 생산자(NF service Producer) 또는 NF 생산자(NF Producer) 또한 동일한 의미이며, 이하의 설명에서 동일한 NF로 설명한다. 따라서 NF 서비스 생산자 또는 NF 생산자가 혼용되더라도 동일한 의미로 이해되어야 할 것이다.

[0049] 도 3을 참조하면, NF 서비스 소비자(300)는 311단계에서 NRF(117)로 액세스 토큰 획득 요청(Access Token Get Request) 메시지를 전송하여 서비스를 받고자 하는 NF Producer의 접근 허가를 요청할 수 있다. 이때, NF Consumer(300)는 Access Token Get Request 메시지에 아래의 정보의 전부 또는 일부 포함할 수 있다.

[0050] - NF Consumer의 NF Instance ID, NF Type

[0051] - 접근 허가를 원하는 NF 서비스에 대한 정보

[0052] - 접근 허가를 원하는 NF Producer의 NF Type 및 NF Producer Instance ID 등의 정보

[0053] 또한, NF Consumer(300)는 Access Token Get Request 메시지에 NF Producer의 서비스를 사용할 때, NF Producer에게서 회신 받고자 하는 주소를 나타내는 NF Consumer의 응답 인터넷 식별자(Response Uniform Resource Identifier(URI))를 포함할 수 있다.

[0054] NRF(117)는 NF Consumer(300)에게서 Access Token Get Request 메시지를 수신한 후, NRF(117)는 312단계에서 NF Consumer(300)가 요청되는 NF Producer의 서비스에 접근이 가능한지 허가 가능 여부를 판단(또는 식별 또는 검색)할 수 있다. 이때, NRF(117)는 이전에 NF Producer가 NRF(117)에게 등록하였거나, 또는 사전에 설정된 정

보 등을 통해서 요청되는 NF Producer가 제공해주는 서비스의 허가 가능한 NF type 또는 NF Instance ID 리스트 등이 존재하는 경우, NRF(117)는 312단계에서 NF Consumer(300)가 해당 리스트에 포함되는 지의 정보를 활용하여 접근 허가를 해주어도 되는 요청인지를 확인할 수 있다.

[0055] 또한, 추가로, NRF(117)는 312단계에서 Access Token Get Request 메시지에 포함된 Response URI가 이전에 NF Consumer(300)가 NRF(117)에 등록하였던 Response URI의 리스트에 들어있는 URI인지 또는, NF Consumer(300)가 등록한 FQDN 또는 IP Address가 가리키는 호스트 주소를 사용하는 URI인지 등을 판단(또는 식별)하여, NF Consumer(300)의 Access Token Get Request 메시지에 포함된 요청이 올바른 요청인지 접근 허가를 해주어도 되는 요청인지 등을 확인(또는 식별)할 수 있다.

[0056] 본 개시의 다른 실시 예로 NF Consumer(300)는 311단계에서 자신의 IP 주소, FQDN 또는 Response URI에 사용될 URI의 정보를 자신의 인증서에 포함할 수 있다. 이에 따라, NRF(117)는 NF Consumer(300)로부터 위와 같은 정보를 포함하는 Access Token Get Request 메시지를 수신할 수 있다. 그러면, NRF(117)는 312단계에서 해당 Access Token Request 메시지에 포함된 Response URI의 정보가 NF Consumer(300)의 인증서에 포함된 Response URI의 리스트에 포함되어 있는 URI인지 또는, 인증서에 포함되어 있는 FQDN 또는 IP Address가 가리키는 호스트 주소를 사용하는 URI인지 등을 판단(또는 식별)하여, NF Consumer(300)의 Access Token Get Request 메시지에 포함된 요청이 올바른 요청인지 접근 허가를 해주어도 되는 요청인지 등을 확인할 수 있다.

[0057] NRF(117)는 NF Consumer(300)의 예상되는 NF Producer의 서비스 사용이 가능하다고 판단된 경우, NRF(117)는 313단계에서 NRF ID, NF Consumer(300)의 NF Instance ID, 요청되는 NF Producer Type, 만일 요청되는 NF Producer instance가 지정되어 있다면 해당 NF Producer의 NF Instance ID 등의 정보를 포함하는 토큰을 NF Consumer(300)에게 발행해 줄 수 있다. 이때, Token은 NRF(117)의 암호 키로 서명될 수 있다.

[0058] 또한, NRF(117)가 발행하는 토큰은 해당 토큰의 유효기간을 알릴 수 있는 시간 정보를 포함할 수 있다.

[0059] 추가로, NRF(117)는 313단계에서 NF Consumer(300)에게 발행해주는 토큰에 NF Consumer(300)의 FQDN 또는 IP Address 그리고 Response URI 등의 정보를 포함하여, NF Producer가 요청되는 응답 URI(Response URI)가 NF Consumer(300)의 올바른 URI인지 확인하게 할 수 있다. 이때, Response URI는 NF Consumer(300)의 Access Token Get Request 메시지에 포함된 Response URI의 정보를 포함할 수 있다. 만일 NF Consumer(300)의 Access Token Get Request 메시지에 Response URI가 포함되지 않은 경우, NRF(117)는 이전에 NF Consumer가 등록하였던 Response URI 리스트의 정보를 전부 또는 일부만 포함할 수 있다.

[0060] NRF(117)는 313단계에서 자신의 암호 키로 서명된 토큰을 포함하여 NF Consumer(300)에게 Access Token Get Request 메시지의 회신을 전송할 수 있다.

[0061] 도 4는 본 개시의 실시 예에 따른 네트워크 장치 인증서를 활용하여 네트워크 장치 간 가입-통지(SUBSCRIBE-NOTIFICATION) 모델의 서비스 요청 및 회신의 인증 및 권한 허가 절차에 대한 신호 흐름도이다.

[0062] 도 4를 참조하여 설명하기에 앞서 본 개시에서 사용되는 네트워크 기능들을 살펴보기로 한다. 먼저 NF Consumer(401)는 NFc_1로 예시하였으며, NF Producer는 서로 다른 2개의 NF Producer가 존재하는 형태를 예시하고 있다. 따라서 제1NF Producer(402)는 NFp_1으로 예시하였으며, 제2NF Producer(403)는 NFp_2로 예시하였다. 또한 도 1에서 설명한 SCP(114)와 NRF(117)의 구성 요소들을 이용하는 경우를 가정한다. 또한 NFp_1은 특정한 경우 제2의 NF Consumer로 동작할 수 있다. 즉, 하나의 NF가 NFp_1로 동작하면서 동시에 특정한 경우에 NFc_2로 동작할 수 있다. 그러므로 도 4에서는 이를 함께 예시하고 있다. 이에 대하여는 도 4의 신호 흐름도를 참조하여 더 살펴보기로 한다.

[0063] 본 개시의 실시 예에 따르면, NF Consumer는 NF Producer의 통지(NOTIFICATION) 서비스에 가입(SUBSCRIPTION)하고 이후에, 별다른 요청 없이 NF Producer에게서 통지 서비스를 수신할 수 있다. 또한, NF Producer는 NF Consumer에게 통지 서비스를 요청 받고 이를 승낙한 후, 해당 요청에 대한 서비스를 제공해주기 위해서 필요한 경우, 다른 NF Producer(도 4의 예시에서 NF Producer_2라고 칭한다)에게 NF Consumer에게 통지 서비스를 제공해주도록 요청할 수 있다. 예를 들어, NEF(116)는 AF의 요청 등에 따라서, NF Consumer로서 특정 단말에 대한 위치의 변경, 네트워크 접속 상태의 변경 등의 이벤트에 대해서 통지 서비스를 제공해주도록 UDM(119)에게 통지 서비스를 요청할 수 있다. 이때, UDM(119)은 해당 통지 서비스의 NF Producer로 동작할 수 있다. 이때, NEF(116)는 UDM(119)에게 통지 서비스를 전송할 NEF(116)의 URI를 Response URI로 같이 등록할 수 있다. UDM(119)은 UE의 네트워크 접속 상태의 변경 등에 이벤트에 대해서 AMF(112)에게서 정보를 얻고자 AMF(112)에게 해당 Event에 대해서 통지 서비스에 가입할 수 있다. 이때, UDM(119)은 또 다른 NF Consumer로서(여기서는 NF

Consumer_2라고 지칭하자) AMF(112)의 통지 서비스에 가입한다. AMF(112)는 NF Producer로서 동작하게 된다(여기서는 NF Consumer_2라고 지칭한다). 이때, UDM(119)은 해당 Event에 대해서는 AMF(112)에게 해당 통지 서비스의 수신자 URI로 NF Consuner_2의 Response URI가 아닌 NF Consumer_1의 Response URI, 즉, NEF(116)에게서 받은 Response URI를 사용할 수 있다.

[0064] 도 4의 실시 예에 따라서 NF Consumer_1(410)은 NF Producer_1(402)에게 특정 UE나 UE의 그룹 등을 대상으로 하는 특정 이벤트에 대해서 통지 서비스 가입을 결정할 수 있다. 이때, 특정 이벤트는 이벤트 지시자(Event ID)로 대표될 수 있다.

[0065] NF Consumer_1(401)은 NF Producer의 통지 서비스 가입 요청을 위해서 411단계에서 서비스 요청(Service Request) 메시지를 전송할 수 있도록 NRF(117)에게서 권한 확인을 수행하고 토큰을 발행 받을 수 있다.

[0066] NF Consumer_1(401)은 412단계에서 Service Request 메시지를 수신하는 NF Producer가 NF Consumer_1(401)을 인증할 수 있도록 NF Consumer_1(401)의 CCA 인증서를 생성할 수 있다.

[0067] NF Consumer_1(401)은 413단계에서와 같이 NF Producer에게 통지 서비스 가입 요청을 위하여 Service Request 메시지를 SCP(114)에게 전송하거나, NF Producer에게 직접 전송(도 4에는 예시하지 않음)할 수 있다. 이때, Service Request 메시지는 요청되는 이벤트를 나타내는 이벤트 지시자, 관련한 UE의 정보를 나타낼 수 있는 UE의 지시자 정보, 그리고, CCA 인증서와 NRF(117)로부터 받은 토큰을 포함할 수 있다.

[0068] 본 개시의 실시 예에서 CCA는 NF Consumer(401)의 NF Instance ID, 인증서의 유효기간을 알릴 수 있는 시간 정보, 예상되는 NF Producer의 NF Type, 그리고 NF Consumer의 디지털 인증서 또는 디지털 인증서의 URL 정보 등을 포함할 수 있다. 또한, Service Request 메시지에 포함된 서비스 요청에 대한 응답 또는 서비스를 제공받고자 하는 NF의 Response URI 정보를 포함할 수 있다. NF의 CCA는 NF의 서명 키로 서명될 수 있다.

[0069] SCP(114)는 414단계에서 NF Consumer_1(401)로부터 수신한 Service Request 메시지를 NF Producer_1(402)에게 전송할 수 있다.

[0070] NF Producer_1(402)은 수신한 Service Request 메시지에 포함된 토큰과 CCA 인증서를 검증하여 Service Request 메시지를 전송한 NF Consumer_1(401)을 인증하고 NRF(117)에서 접근 허가를 받은 NF인지 확인할 수 있다. 또한, NF Producer_1(402)은 415단계를 통해 Service Request 메시지에 포함된 Response URI와 CCA 인증서에 첨부된 Response URI가 NF Consumer_1(401)의 URI임을 확인할 수 있다.

[0071] 본 개시의 다른 실시 예로 NF Producer의 디지털 인증서에 FQDN 또는 IP Address가 포함된 경우, NF Producer_1(402)은 Service Request 메시지 및 CCA에 포함된 Response URI가 FQDN 또는 IP Address이 가리키는 호스트 주소를 사용하는 지 확인하여 NF Consumer_1(401)에서의 Service Request 메시지가 올바른 Service Request 메시지인지 확인할 수 있다.

[0072] NF Producer_1(402)은 NF Consumer_1(401)에게서 수신한 Service Request 메시지에 포함된 이벤트에 대한 통지 서비스를 제공해주기 위해서 다른 NF Producer인 NF Producer_2(403))에게 해당 이벤트에 대한 통지 서비스를 요청해야 함을 결정할 수 있다.

[0073] NF Producer_1(402)은 NF Consumer로서(여기서는 NF Consumer_2라고 지칭하자), 415단계에서 NF Producer_2(403)에게 서비스 요청을 위하여 NRF(117)에게 토큰을 요청할 수 있다. 이때, 토큰 요청에는 NF Consumer_2 ID, 요구되는 NF Producer_2의 NF type, 요구되는 NF 서비스 정보 등을 포함할 수 있다.

[0074] NF Consumer_2(402)은 NRF(117)에게서 토큰을 받은 후, 416단계에서 NF Producer_2(403)에게 통지 서비스 가입 요청을 위하여 Service Request 메시지를 구성하고 417단계에서 이를 SCP(114)에게 전송하거나, 또는 NF Producer_2(403)에게 직접 전송할 수 있다(직접 전송의 경우 도 4에 예시하지 않음). 이때, Service Request 메시지는 요청되는 이벤트를 나타내는 이벤트 지시자, 이벤트와 관련한 UE의 정보를 나타낼 수 있는 UE의 지시자 정보, 그리고, CCA 인증서와 NRF(117)에게서 받은 토큰을 포함할 수 있다.

[0075] 이때, NF Consumer_2(402)는 NF Consumer_1(401)에게서 요청 받은 이벤트와 연관된 NF Producer_2(403)에서 통지 서비스를 제공해 줄 수 있는 이벤트에 대해서 통지 서비스를 받을 수 있는 주소로 NF Consumer_1(401)의 Response URI를 Service Request 메시지에 포함할 수 있다. 만일, NF Consumer_2(402)가 NF Producer_2(403)에게 요청되는 통지 서비스의 가입 요청을 위한 Service Request 메시지에 NF Consumer_1(401)의 Response URI를 포함시킨 경우, NF Consumer_2(402)는 해당 Response URI의 주인인 NF Consumer_1(401)을 확인시켜 주기 위해

서 NF Consumer_1에게서 수신한 NF_Consumer_1(401)의 CCA 인증서를 같이 첨부할 수 있다.

[0076] SCP(114)는 418단계에서 NF Consumer_2(402)에게서 수신한 Service Request 메시지를 NF Producer_2(403)에게 전송할 수 있다.

[0077] NF Producer_2(403)는 420단계에서 NF Consumer_2(402)로부터 수신한 Service Request 메시지와 그 안에 포함된 NF Consumer_1(401)의 Response URI 등을 검증하고, 해당 Service 요청이 적정한 요청인 경우 421단계에서 해당 Service Request 메시지에 대한 승인을 회신할 수 있다.

[0078] 이때, NF Producer_2(403)은 402단계에서 수신한 Service Request 메시지에 포함된 토큰과 NF Consumer_2(402)의 CCA 인증서를 검증하여 Service Request 메시지를 전송한 NF Consumer_2(402)를 인증 확인 및 NRF(117)에서 접근 허가를 받은 NF 인지 허가 여부를 확인할 수 있다. 또한, NF Producer_2(403)은 Service Request 메시지에 포함된 Response URI와, 같이 첨부된 NF Consumer_1(401)의 CCA 인증서를 확인하여 해당 Response URI의 주인이 NF Consumer_1(401)인지 인증하고, NF Consumer_1(401)이 NF Producer_2(402)가 제공해주는 해당 이벤트의 통지 서비스를 수신할 수 있는 NF인지의 권한 허가 확인을 할 수 있다.

[0079] 이때, NF Producer_2(403)는 상기 통지 서비스 가입이 성공한 경우, 해당 UE에 대한 이벤트 발생 시, Response URI로 통지 서비스를 제공해 주기 위해서, 요청받은 UE의 정보와 해당되는 Event ID, 그리고 Response URI를 저장할 수 있다.

[0080] 만일 상기 언급된 NF Consumer_1(401)이 통지 서비스를 받을 수 있는 권한이 없는 NF Type이거나, 올바른 NF로 인증 받지 못한 경우 등의 여러 경우로 해당 요청이 승인할 수 없는 경우, NF Producer_2(403)는 해당 요청을 거절할 수 있다.

[0081] NF Producer_2(403)에서의 서비스 응답(Service Response) 메시지는 421단계, 422단계와 같이 SCP(114)를 거치거나 또는, 직접 NF Consumer_2(402)에게 전송될 수 있다.

[0082] 성공적인 Service Response 메시지를 수신한 NF Consumer_2(NF Producer_1과 동일한 NF)(402)는 423단계 및 424단계를 통해 NF Consumer_1(401)의 Service Request 메시지를 회신할 수 있다.

[0083] 본 개시의 다른 실시 예로 NF Producer_1(402)은 NF Consumer_1(402)에서의 Service Request 메시지를 수신하고 NF Consumer_1(401)의 권한 검증을 성공한 후, NF Producer_2(403)와 주고 받는 Service Request 메시지와 상관없이 NF Consumer_1(401)에게 Service Response를 회신할 수 있다.

[0084] NF Producer_2(403)는 요청받은 단말에 대한 상기 요청받은 Event가 발생 시, 425단계 및 426단계와 같이 저장해 두었던 Response URI를 활용하여 NF Consumer_1(401)에게 통지 서비스를 제공할 수 있다. 이때, 통지 서비스는 NF Consumer_1(401)에게 직접 전송(도 4에서는 예시하지 않음)되거나, SCP를 통해서 전송될 수 있다.

[0085] 도 5는 본 개시의 실시 예에 따른 네트워크 장치의 시스템 등록 정보를 활용한 네트워크 장치 간 SUBSCRIBE-NOTIFICATION 모델의 서비스 요청 및 회신의 인증 및 권한 허가 절차에 따른 신호 흐름도이다.

[0086] 도 5를 참조하여 설명하기에 앞서 각 NF들에 대하여 도 4에서 사용된 참조부호들을 그대로 사용할 것이다. 따라서 도 4에서 가정한 형태가 도 5에서도 적용될 수 있다.

[0087] 본 개시의 실시 예에서 NF들은 NF 등록 과정을 통해서 사전에 NF의 FQDN 또는 IP Address을 NRF(117)에 등록할 수 있다(510단계). 이때, NF들은 FQDN 또는 IP Address에 더해서 NF의 Response URI 정보들을 NRF(117)에 등록할 수 있다.

[0088] 본 개시의 실시 예에 따라서 NF Consumer_1(401)은 NF Producer_1(402)에게 특정 UE나 UE의 그룹 등을 대상으로 하는 특정 이벤트에 대해서 통지 서비스 가입을 결정할 수 있다. 이때, 특정 이벤트는 이벤트 지시자(Event ID)로 대표될 수 있다.

[0089] NF Consumer_1(401)은 511단계에서 NF Producer의 통지 서비스 가입 요청을 위해서 Service Request 메시지를 전송할 수 있도록 NRF(117)에게서 권한 확인을 수행하고 토큰을 발행 받기 위하여 Access Token Request 메시지를 전송할 수 있다. 이때, Access Token Request 메시지는 아래의 정보들을 전부 또는 일부 포함할 수 있다.

[0090] - NF Consumer의 NF Instance ID, NF Type

[0091] - 접근 허가를 원하는 NF 서비스에 대한 정보

[0092] - 접근 허가를 원하는 NF Producer의 NF Type 및 NF Producer Instance ID 등의 정보

[0093] 또한, NF Consumer는 Access Token Get Request 메시지에 NF Producer의 서비스를 사용할 때, NF Producer에게서 회신 받고자 하는 주소를 나타내는 NF Consumer의 Response URI를 포함할 수 있다.

[0094] NRF(117)는 512단계에서 Access Token Request 메시지에 포함된 정보 및 예상되는 NF Producer가 지정한 정보(예를 들어, 서비스를 받을 수 있는 NF Consumer의 NF type 등)를 활용하여 해당 토큰 요청에 대한 권한 허가를 결정하고 토큰을 발행할 수 있다. 이때, NRF(117)는 Access Token Request 메시지에 포함된 Response URI와 기존에 등록된 NF Consumer_1의 FQDN 또는 IP Address 또는 Response URI의 정보를 비교하여 해당 요청이 올바른 요청인지 확인하고 권한 허가를 결정할 수 있다.

[0095] NRF(117)는 513단계에서 발행된 토큰 정보를 포함하는 서비스 응답(service response) 메시지를 NF Consumer_1(401)로 전송할 수 있다.

[0096] NF Consumer_1(401)은 NF Producer_1(402)에게 통지 서비스 가입 요청을 위하여 515단계에서 Service Request 메시지를 SCP에게 전송하거나, NF Producer_1(402)에게 직접 전송(도 5에 예시하지 않음)할 수 있다. 이때, Service Request 메시지는 요청되는 이벤트를 나타내는 이벤트 지시자, 관련한 UE의 정보를 나타낼 수 있는 UE의 지시자 정보, 그리고, CCA 인증서와 NRF에게서 받은 토큰을 포함할 수 있다.

[0097] 본 개시의 실시 예에서 CCA는 NF Consumer의 NF Instance ID, 인증서의 유효기간을 알릴 수 있는 시간 정보, 예상되는 NF Producer의 NF Type, 그리고 NF Consumer의 디지털 인증서 또는 디지털 인증서의 URL 정보 등을 포함할 수 있다. NF의 CCA는 NF의 서명 키로 서명될 수 있다.

[0098] SCP(114)는 515단계에서 NF Consumer_1(401)로부터 수신한 Service Request 메시지를 NF Producer_1(402)에게 전송 한다.

[0099] NF Producer_1(402)은 516단계에서 수신한 Service Request 메시지에 포함된 토큰과 CCA 인증서를 검증하여 Service Request 메시지를 전송한 NF Consumer_1(401)을 인증하고 NRF(117)에서 접근 허가를 받은 NF인지를 확인할 수 있다.

[0100] 본 개시의 다른 실시 예로 NF Producer의 디지털 인증서에 FQDN 또는 IP Address이 포함된 경우, Service Request 및 CCA에 포함된 Response URI가 FQDN 또는 IP Address이 가리키는 호스트 주소를 사용하는지 확인하여 NF Consumer_1(401)에서의 Service Request 메시지가 올바른 Service Request 메시지인지를 확인할 수 있다.

[0101] NF Producer_1(402)은 NF Consumer_1(401)로부터 수신한 Service Request 메시지에 포함된 이벤트에 대한 통지 서비스를 제공해주기 위해서 다른 NF Producer (여기서는 NF Producer_2)에게 해당 이벤트에 대한 통지 서비스를 요청해야 함을 결정할 수 있다.

[0102] NF Producer_1(402)은 NF Consumer로서(여기서는 NF Consumer_2라고 지칭하자), 517단계와 같이 NF Producer_2(403)에게 서비스 요청을 위하여 NRF(117)에게 토큰을 요청할 수 있다. 이때, 토큰 요청에는 NF Consumer_2 ID, 요구되는 NF Producer_2의 NF type, 요구되는 NF 서비스 정보 등을 포함할 수 있다. 또한, NF Consumer_2(402)는 NF_Consumer_1(401)에게서 받은 Response URI를 NF Producer_2(403)에서의 통지 서비스를 받고자 하는 주소로 토큰 요청에 추가할 수 있다. 이때, NF Consumer_2(402)는 NRF(117)에게 해당 Response URI가 NF Consumer_1(401)에게서 수신한 것임을 알릴 수 있는 NF Consumer_1(401)에게서 수신한 CCA 또는 NF Consumer_1(401)의 NF Instance ID의 정보를 포함할 수 있다.

[0103] NRF(117)는 518단계에서 Access Token Request 메시지에 포함된 정보 및 예상되는 NF Producer가 지정한 정보 등을 활용하여 해당 토큰 요청에 대한 권한 허가를 결정하고 519단계와 같이 토큰을 발행할 수 있다. 이때, NRF(117)는 Access Token Request 메시지에 포함된 NF Consumer_1(401)의 Response URI와 Access Token Request 메시지에 포함된 NF Consumer_1(401)의 CCA 정보 또는 NF Instance ID 정보에서 NF Consumer_1(401)을 확인하고, 기존에 등록된 NF Consumer_1(401)의 FQDN 또는 IP Address 또는 Response URI의 정보를 비교하여 해당 요청이 올바른 요청인지 확인하고 NF Consumer_1(401)이 NF Producer_2(403)의 통지 서비스를 수신할 수 있는지 권한 허가를 결정할 수 있다. 이때, NRF(117)는 NF Consumer_2에게 요청 받은 대로 NF Consumer_1(401)의 Response URI를 토큰에 포함할 수 있다.

[0104] NF Consumer_2(402)은 NRF(117)에게서 토큰을 받은 후, NF Producer_2(430)에게 통지 서비스 가입 요청을 위하여 Service Request 메시지를 구성하고 520단계와 같이 이를 SCP(114)에게 전송하거나, 또는 NF

Producer_2(403)에게 직접 전송(도 5에 예시하지 않음)할 수 있다. 이때, Service Request 메시지는 요청되는 이벤트를 나타내는 이벤트 지시자, 이벤트와 관련한 단말의 정보를 나타낼 수 있는 UE의 지시자 정보, 그리고, CCA 인증서와 NRF에게서 받은 토큰을 포함할 수 있다.

[0105] 이때, NF Consumer_2(402)는 NF Consumer_1(401)에게서 요청 받은 이벤트와 연관된 이벤트 중에서 NF Producer_2(403)에서 통지 서비스를 제공해 줄 수 있는 이벤트에 대해서 통지 서비스를 받을 수 있는 주소로 NF Consumer_1의 Response URI를 Service Request에 포함할 수 있다.

[0106] SCP(114)는 521단계에서 NF Consumer_2(402)로부터 수신한 Service Request 메시지를 NF Producer_2(403)에게 전송할 수 있다.

[0107] NF Producer_2(403)는 522단계에서 NF Consumer_2(402)에서 수신한 Service Request 메시지와 그 안에 포함된 토큰과 NF Consumer_2(402)의 CCA 인증서를 검증하여 Service Request 메시지를 전송한 NF Consumer_2(402)를 인증 확인 및 NRF(117)에서 접근허가를 받은 NF인지 허가 여부를 확인할 수 있다. 이때, 추가로, NF Producer_2(403)는 해당 Response URI가 NRF(117)에게서 인증 및 허가를 받은 URI인 것을 확인하고 상기 절차들을 수행하여 해당 Service Request 메시지가 적정한 요청인지 확인할 수 있다.

[0108] NF Producer_2(403)는 NF Consumer_2(402)의 Service 요청이 적정한 요청인 경우 523단계와 같이 해당 Service Request 메시지에 대한 승인을 회신할 수 있다.

[0109] 이때, NF Producer_2(403)는 상기 통지 서비스 가입이 성공한 경우, 해당 UE에 대한 이벤트 발생 시, Response URI로 통지 서비스를 제공해 주기 위해서, 요청 받은 UE의 정보와 해당되는 Event ID, 그리고 Response URI를 저장한다.

[0110] 만일 상기 언급된 NF Consumer_1(401)이 통지 서비스를 받을 수 있는 권한이 없는 NF Type이거나, 올바른 NF로 인증 받지 못한 경우 등의 여러 경우로 해당 요청이 승인할 수 없는 경우, NF Producer_2(403)는 해당 요청을 거절할 수 있다.

[0111] NF Producer_2(403)에서의 Service Response 메시지는 523단계 및 525단계로 예시한 바와 같이 SCP(114)를 거치거나 또는, 직접 NF Consumer_2(402)에게 전송(도 5에 예시하지 않음)될 수 있다.

[0112] 성공적인 Service Response 메시지를 수신한 NF Consumer_2(NF Producer_1과 동일한 NF)(402)는 526단계 및 527단계와 같이 NF Consumer_1(401)의 Service Request에 회신으로, 서비스 응답 메시지를 NF Consumer_1(401)로 전송할 수 있다.

[0113] 본 개시의 다른 실시 예로 NF Producer_1(402)은 NF Consumer_1(401)에서의 Service Request 메시지를 수신하고 NF Consumer_1(401)의 권한 검증을 성공한 후, NF Producer_2(403)와 주고 받는 Service Request 메시지와 상관없이 NF Consumer_1(401)에게 Service Response 메시지를 회신할 수 있다.

[0114] NF Producer_2(402)는 요청받은 UE에 대한 상기 요청받은 Event가 발생 시, 528단계 및 529단계와 저장해 두었던 Response URI를 활용하여 NF Consumer_1(401)에게 통지 서비스를 제공할 수 있다. 이때, 통지 서비스는 NF Consumer_1(401)에게 직접 전송(도 5에는 예시하지 않음)되거나, 도 5의 528단계 및 529단계와 같이 SCP(114)를 통해서 전송될 수 있다.

[0115] 도 6은 본 개시의 실시 예에 따른 네트워크 장치의 인증서 정보를 활용한 네트워크 장치 간 SUBSCRIBE-NOTIFICATION 모델의 서비스 요청 및 회신의 인증 및 권한 허가 절차에 따른 신호 흐름도이다.

[0116] 도 6을 참조하여 설명하기에 앞서 각 NF들에 대하여 도 4에서 사용된 참조부호들을 그대로 사용할 것이다. 따라서 도 4에서 가정한 형태가 도 6에서도 적용될 수 있다.

[0117] 본 개시의 실시 예에서 NF들은 610단계와 같이 NF의 디지털 인증서에 NF의 FQDN 또는 IP Address를 포함할 수 있다. 또한, NF들은 추가로 NF의 Response URI 정보들을 디지털 인증서에 포함할 수 있다.

[0118] 본 개시의 실시 예에 따라서 NF Consumer_1(401)은 NF Producer_1(402)에게 특정 UE 또는 UE의 그룹 등을 대상으로 하는 특정 이벤트에 대해서 통지 서비스 가입을 결정할 수 있다. 이때, 특정 이벤트는 이벤트 지시자(Event ID)로 대표될 수 있다.

[0119] NF Consumer_1(401)은 NF Producer의 통지 서비스 가입 요청을 위해서 611단계에서 Service Request 메시지를 전송할 수 있도록 NRF(117)에게서 권한 확인을 수행하고 토큰을 발행 받기 위하여 Access Token Request 메시지

를 전송할 수 있다. 이때, Access Token Request 메시지는 아래의 정보들을 전부 또는 일부 포함할 수 있다.

[0120] - NF Consumer의 NF Instance ID, NF Type

[0121] - 접근 허가를 원하는 NF 서비스에 대한 정보

[0122] - 접근 허가를 원하는 NF Producer의 NF Type 및 NF Producer Instance ID 등의 정보

[0123] 또한, NF Consumer는 Access Token Get Request 메시지에 NF Producer의 서비스를 사용할 때, NF Producer에게서 회신 받고자 하는 주소를 나타내는 NF Consumer의 Response URI를 포함할 수 있다.

[0124] NRF(117)는 612단계에서 Access Token Request에 포함된 정보 및 예상되는 NF Producer가 지정한 정보(예를 들어, 서비스를 받을 수 있는 NF Consumer의 NF type 등)를 활용하여 해당 토큰 요청에 대한 권한 허가를 결정하고, 613단계와 같이 토큰을 발행할 수 있다. 이때, NRF(117)는 Access Token Request 메시지에 포함된 Response URI와 NF의 인증서에 포함된 FQDN 또는 IP Address 또는 Response URI의 정보를 비교하여 해당 요청이 올바른 요청인지 확인하고 권한 허가를 결정할 수 있다.

[0125] NF Consumer_1(401)은 614단계와 같이 NF Producer_1(401)에게 통지 서비스 가입 요청을 위하여 Service Request 메시지를 SCP(114)에게 전송하거나, NF Producer_1(402)에게 직접 전송(도 5에 예시하지 않음)할 수 있다. 이때, Service Request 메시지는 요청되는 이벤트를 나타내는 이벤트 지시자, 관련한 UE의 정보를 나타낼 수 있는 UE의 지시자 정보, 그리고, CCA 인증서와 NRF(117)에게서 받은 토큰을 포함할 수 있다.

[0126] 본 개시의 실시 예에서 CCA는 NF Consumer의 NF Instance ID, 인증서의 유효기간을 알릴 수 있는 시간 정보, 예상되는 NF Producer의 NF Type, 그리고 NF Consumer의 디지털 인증서 또는 디지털 인증서의 URL 정보 등을 포함할 수 있다. NF의 CCA는 NF의 서명 키로 서명될 수 있다.

[0127] SCP(114)는 NF Consumer_1(401)로부터 수신한 Service Request 메시지를 615단계에서 NF Producer_1(402)에게 전송할 수 있다.

[0128] NF Producer_1(402)은 616단계에서 수신한 Service Request 메시지에 포함된 토큰과 CCA 인증서를 검증하여 Service Request 메시지를 전송한 NF Consumer_1(401)을 인증하고 NRF(117)에서 접근 허가를 받은 NF인지 확인할 수 있다.

[0129] 본 개시의 다른 실시 예로 NF Producer의 디지털 인증서에 FQDN 또는 IP Address가 포함된 경우, Service Request 메시지 및 CCA에 포함된 Response URI가 FQDN 또는 IP Address가 가리키는 호스트 주소를 사용하는지 확인하여 NF Consumer_1(401)에서의 Service Request 메시지가 올바른 Service Request 메시지인지 확인할 수 있다.

[0130] NF Producer_1(402)은 NF Consumer_1(401)로부터 수신한 Service Request 메시지에 포함된 이벤트에 대한 통지 서비스를 제공해주기 위해서 다른 NF Producer(여기서는 NF Producer_2)(403)에게 해당 이벤트에 대한 통지 서비스를 요청해야 함을 결정할 수 있다.

[0131] NF Producer_1(402)은 NF Consumer로서(여기서는 NF Consumer_2라고 지칭하자), NF Producer_2(403)에게 서비스 요청을 위하여 617단계와 같이 NRF(117)에게 토큰을 요청할 수 있다. 이때, 토큰 요청에는 NF Consumer_2 ID, 요구되는 NF Producer_2의 NF type, 요구되는 NF 서비스 정보 등을 포함할 수 있다. 또한, NF Consumer_2(402)는 NF_Consumer_1(401)에게서 받은 Response URI를 NF Producer_2(403)에서의 통지 서비스를 받고자 하는 주소로 토큰 요청에 추가할 수 있다. 이때, NF Consumer_2(402)는 NRF(117)에게 해당 Response URI가 NF Consumer_1에게서 수신한 것임을 알릴 수 있는 NF Consumer_1에게서 수신한 CCA 의 정보를 포함할 수 있다.

[0132] NRF(117)는 618단계에서 Access Token Request 메시지에 포함된 정보 및 예상되는 NF Producer가 지정한 정보 등을 활용하여 해당 토큰 요청에 대한 권한 허가를 결정하고, 619단계와 같이 토큰을 발행할 수 있다. 이때, NRF(117)는 Access Token Request 메시지에 포함된 NF Consumer_1(401)의 Response URI와 Access Token Request 메시지에 포함된 NF Consumer_1(401)의 CCA 정보에서 NF Consumer_1(401)을 확인하고, NF Consumer_1의 디지털 인증서에 등록된 NF Consumer_1(401)의 FQDN 또는 IP Address 또는 Response URI의 정보를 비교하여 해당 요청이 올바른 요청인지 확인하고 NF Consumer_1(401)이 NF Producer_2(403)의 통지 서비스를 수신할 수 있는지 권한 허가를 결정할 수 있다. 이때, NRF(117)는 NF Consumer_2(402)에게 요청 받은 대로 NF Consumer_1(401)의 Response URI를 토큰에 포함할 수 있다.

[0133] NF Consumer_2(402)은 NRF(117)에게서 619단계와 같이 토큰을 받은 후, NF Producer_2(403)에게 통지 서비스 가입 요청을 위하여 Service Request 메시지를 구성하고 420단계와 같이 이를 SCP(114)에게 전송하거나, 또는 NF Producer_2(403)에게 직접 전송(도 6에 예시하지 않음)할 수 있다. 이때, Service Request 메시지는 요청되는 이벤트를 나타내는 이벤트 지시자, 이벤트와 관련한 단말의 정보를 나타낼 수 있는 UE의 지시자 정보, 그리고, CCA 인증서와 NRF(117)에게서 받은 토큰을 포함할 수 있다.

[0134] 본 개시의 다른 실시 예로 NF Consumer_2(4032)는 Service Request 메시지에 포함된 Response URI의 확인을 위해서 NF Consumer_1(401)의 CCA 인증서 또는 NF Consumer_1의 디지털 인증서 또는 디지털 인증서 URL 등의 정보를 상기 Service Request 메시지에 추가할 수 있다.

[0135] 이때, NF Consumer_2(402)는 NF Consumer_1(401)에게서 요청 받은 이벤트와 연관된 이벤트 중에서 NF Producer_2(403)에서 통지 서비스를 제공해 줄 수 있는 이벤트에 대해서 통지 서비스를 받을 수 있는 주소로 NF Consumer_1(401)의 Response URI를 Service Request 메시지에 포함할 수 있다.

[0136] SCP(114)는 NF Consumer_2(402)로부터 수신한 Service Request를 421단계에서 NF Producer_2(403)에게 전송할 수 있다.

[0137] NF Producer_2(403)는 622단계에서 NF Consumer_2(402)로부터 수신한 Service Request 메시지와 그 안에 포함된 토큰과 NF Consumer_2(402)의 CCA 인증서를 검증하여 Service Request 메시지를 전송한 NF Consumer_2(402)을 인증 확인 및 NRF(117)에서 접근 허가를 받은 NF인지 허가 여부를 확인할 수 있다. 이때, 추가로, NF Producer_2(403)는 해당 Response URI가 NRF(117)에게서 인증 및 허가를 받은 URI인 것을 확인하고 상기 절차들을 수행하여 해당 Service Request가 적정한 요청인지 확인할 수 있다.

[0138] 또한, NF Producer_2(403)는 622단계에서 NF Consumer_1(401)의 CCA 인증서, 또는 디지털 인증서 또는 디지털 인증서의 URL이 포함된 경우, 상기 인증서의 확인을 통해서 NF Consumer_1(401)을 확인하고 NF Consumer_1(401)의 인증서에 포함된 FQDN 또는 IP Address 또는 Response URI의 정보와 Service Request 메시지에 포함된 Response URI를 비교하여, 해당 Response URI가 NF Consumer_1(401)의 Response URI인지 확인하고, NF Consumer_1(401)이 NF Producer_2(403)의 통지 서비스를 수신할 수 있는지의 권한 허가 여부의 검토 등을 해당 Service Request 요청이 적정한 요청인지 판단(또는 식별)하는데 활용할 수 있다.

[0139] NF Producer_2(403)는 NF Consumer_2(402)의 Service 요청이 적정한 요청인 경우 623단계. 624단계, 625단계 및 626단계와 같이 해당 Service Request 메시지에 대한 승인을 회신할 수 있다.

[0140] 이때, NF Producer_2(403)는 상기 통지 서비스 가입이 성공한 경우, 해당 UE에 대한 이벤트 발생 시, Response URI로 통지 서비스를 제공해 주기 위해서, 요청 받은 UE의 정보와 해당되는 Event ID, 그리고 Response URI를 저장한다.

[0141] 만일 상기 언급된 NF Consumer_1(401)이 통지 서비스를 받을 수 있는 권한이 없는 NF Type이거나, 올바른 NF로 인증 받지 못한 경우 등의 여러 경우로 해당 요청이 승인할 수 없는 경우, NF Producer_2(403)는 해당 요청을 거절할 수 있다.

[0142] NF Producer_2(403)에서의 Service Response 메시지는 위에서 설명한 623단계와 같이 SCP(114)를 거치거나 또는, 직접 NF Consumer_2(402)에게 전송될(도 6에는 예시하지 않음) 수 있다.

[0143] 성공적인 Service Response 메시지를 수신한 NF Consumer_2(NF Producer_1과 동일한 NF)(402)는 625단계 및 626단계와 같이 NF Consumer_1(401)의 Service Request에 대응한 응답으로, 서비스 응답 메시지를 회신할 수 있다.

[0144] 본 개시의 다른 실시 예로 NF Producer_1(402)은 NF Consumer_1(401)에서의 Service Request 메시지를 수신하고 NF Consumer_1(401)의 권한 검증을 성공한 후, NF Producer_2(403)와 주고 받는 Service Request 메시지와 상관없이 NF Consumer_1(401)에게 Service Response 메시지를 회신할 수 있다.

[0145] NF Producer_2(403)는 요청받은 UE에 대한 상기 요청받은 Event가 발생 시, 627eksrPdptj 저장해 두었던 Response URI를 활용하여 NF Consumer_1(401)에게 통지 서비스를 제공할 수 있다. 이때, 통지 서비스는 NF Consumer_1(401)에게 직접 전송(도 6에는 예시하지 않음)되거나, 627단계 및 628단계와 같이 SCP(114)를 통해서 전송될 수 있다.

[0146] 도 7은 본 개시의 실시 예에 따른 네트워크 장치의 토큰 발행 정보를 활용하여, 네트워크 장치 간 SUBSCRIBE-

NOTIFICATION 모델의 서비스 요청 및 회신의 인증 및 권한 허가 절차에 따른 신호 흐름도이다.

[0147] 도 7을 참조하여 설명하기에 앞서 각 NF들에 대하여 도 4에서 사용된 참조부호들을 그대로 사용할 것이다. 따라서 도 4에서 가정한 형태가 도 7에서도 적용될 수 있다.

[0148] 본 개시의 실시 예에 따라서 NF Consumer_1(401)은 NF Producer_1(402)에게 특정 UE 또는 UE의 그룹 등을 대상으로 하는 특정 이벤트에 대해서 통지 서비스 가입을 결정할 수 있다. 이때, 특정 이벤트는 이벤트 지시자(Event ID)로 대표될 수 있다.

[0149] NF Consumer_1(401)은 711단계에서 NF Producer의 통지 서비스 가입 요청을 위해서 Service Request 메시지를 전송할 수 있도록 NRF(117)에게서 권한 확인을 수행하고 토큰을 발행 받기 위하여 Access Token Request 메시지를 전송할 수 있다. 이때, Access Token Request 메시지는 아래의 정보들을 전부 또는 일부 포함할 수 있다.

[0150] - NF Consumer의 NF Instance ID, NF Type

[0151] - 접근 허가를 원하는 NF 서비스에 대한 정보

[0152] - 접근 허가를 원하는 NF Producer의 NF Type 및 NF Producer Instance ID 등의 정보

[0153] 또한, NF Consumer는 Access Token Get Request 메시지에 NF Producer의 서비스를 사용할 때, NF Producer에게서 회신 받고자 하는 주소를 나타내는 NF Consumer의 Response URI를 포함할 수 있다.

[0154] NRF(117)는 712단계에서 Access Token Request 메시지에 포함된 정보 및 예상되는 NF Producer가 지정한 정보(예를 들어, 서비스를 받을 수 있는 NF Consumer의 NF type 등)를 활용하여 해당 토큰 요청에 대한 권한 허가를 결정하고, 713단계와 같이 토큰을 발행할 수 있다.

[0155] 이때, NRF(117)는 Access Token Request 메시지에 포함된 Response URI가 해당 NF Consumer의 FQDN 또는 IP Address과 비교하여 NF Consumer의 Response URI인지 확인할 수 있다. 또한, Response URI가 NF Consumer_1(401)의 올바른 Response URI로 판단된 경우, 일정 기간 동안 해당 정보를 저장해 놓을 수 있다.

[0156] NF Consumer_1(401)은 714단계에서 NF Producer_1(402)에게 통지 서비스 가입 요청을 위하여 Service Request 메시지를 SCP(114)에게 전송하거나, NF Producer_1(402)에게 직접 전송(도 7에 예시하지 않음)할 수 있다. 이때, Service Request 메시지는 요청되는 이벤트를 나타내는 이벤트 지시자, 관련한 UE의 정보를 나타낼 수 있는 UE의 지시자 정보, 그리고, CCA 인증서와 NRF(117)에게서 받은 토큰을 포함할 수 있다.

[0157] 본 개시의 실시 예에서 CCA는 NF Consumer의 NF Instance ID, 인증서의 유효기간을 알릴 수 있는 시간 정보, 예상되는 NF Producer의 NF Type, 그리고 NF Consumer의 디지털 인증서 또는 디지털 인증서의 URL 정보 등을 포함할 수 있다. NF의 CCA는 NF의 서명 키로 서명되어 있다.

[0158] SCP(114)는 715단계에서 NF Consumer_1(401)로부터 수신한 Service Request 메시지를 NF Producer_1(402)에게 전송 한다.

[0159] NF Producer_1(402)은 718단계에서 수신한 Service Request 메시지에 포함된 토큰과 CCA 인증서를 검증하여 Service Request 메시지를 전송한 NF Consumer_1(401)을 인증하고 NRF(117)에서 접근 허가를 받은 NF인지 확인할 수 있다.

[0160] 또한, NF Producer_1(402)은 Service Request 메시지에 포함된 Response URI와 토큰에 포함된 Response URI의 정보를 비교하여, Service Request 메시지가 올바른 요청인지 판정하는데 활용할 수 있다.

[0161] NF Producer_1(402)은 NF Consumer_1(401)로부터 수신한 Service Request 메시지에 포함된 이벤트에 대한 통지 서비스를 제공해주기 위해서 다른 NF Producer(여기서는 NF Producer_2)(403)에게 해당 이벤트에 대한 통지 서비스를 요청해야 함을 결정할 수 있다.

[0162] NF Producer_1(402)은 NF Consumer로서(여기서는 NF Consumer_2라고 지칭하자), 717단계에서 NF Producer_2(403)에게 서비스 요청을 위하여 NRF(117)에게 토큰을 요청할 수 있다. 이때, 토큰 요청에는 NF Consumer_2 ID, 요구되는 NF Producer_2의 NF type, 요구되는 NF 서비스 정보 등을 포함할 수 있다. 또한, NF Consumer_2(402)는 NF_Consumer_1(401)로부터 받은 Response URI를 NF Producer_2(403)에서의 통지 서비스를 받고자 하는 주소로 토큰 요청에 추가할 수 있다. 이때, NF Consumer_2(402)는 NRF(117)에게 해당 Response URI가 NF Consumer_1(401)에게서 수신한 것임을 알릴 수 있는 NF Consumer_1(401)에게서 수신한 CCA의 정보를 포함할 수 있다.

[0163] NRF(117)는 718단계에서 Access Token Request 메시지에 포함된 정보 및 예상되는 NF Producer가 지정한 정보 등을 활용하여 해당 토큰 요청에 대한 권한 허가를 결정하고, 719단계와 같이 토큰을 발행할 수 있다. 이때, NRF(117)는 Access Token Request 메시지에 포함된 NF Consumer_1(401)의 Response URI와 이전에 NRF(117)가 저장해 놓았던 NF Consumer_1(401)의 Response URI가 동일한 URI인지 비교하여 해당 요청이 올바른 요청인지 확인하고 NF Consumer_1(401)이 NF Producer_2(403)의 통지 서비스를 수신할 수 있는지 권한 허가를 결정할 수 있다. 이때, NRF(117)는 NF Consumer_2(402)에게 요청 받은 대로 NF Consumer_1(401)의 Response URI를 토큰에 포함할 수 있다.

[0164] NF Consumer_2(402)은 NRF(117)에게서 토큰을 받은 후, NF Producer_2에게 통지 서비스 가입 요청을 위하여 Service Request 메시지를 구성하고 720단계에서 이를 SCP(114)에게 전송하거나, 또는 NF Producer_2(403)에게 직접 전송(도 7에 예시하지 않음)할 수 있다. 이때, Service Request 메시지는 요청되는 이벤트를 나타내는 이벤트 지시자, 이벤트와 관련한 UE의 정보를 나타낼 수 있는 UE의 지시자 정보, 그리고, CCA 인증서와 NRF(117)에게서 받은 토큰을 포함할 수 있다.

[0165] 이때, NF Consumer_2(402)는 NF Consumer_1(401)에게서 요청 받은 이벤트와 연관된 이벤트 중에서 NF Producer_2(403)에서 통지 서비스를 제공해 줄 수 있는 이벤트에 대해서 통지 서비스를 받을 수 있는 주소로 NF Consumer_1(401)의 Response URI를 Service Request 메시지에 포함할 수 있다.

[0166] SCP(114)는 721단계에서 NF Consumer_2(402)로부터 수신한 Service Request 메시지를 NF Producer_2(403)에게 전송할 수 있다.

[0167] NF Producer_2(403)는 721단계에서 NF Consumer_2(402)로부터 수신한 Service Request 메시지와 그 안에 포함된 토큰과 NF Consumer_2(402)의 CCA 인증서를 검증하여 Service Request 메시지를 전송한 NF Consumer_2(402)의 인증 확인 및 NRF(117)로부터 접근 허가를 받은 NF인지 허가 여부를 확인할 수 있다. 이때, 추가로, NF Producer_2(403)는 해당 Response URI가 NRF(117)에게서 인증 및 허가를 받은 URI인 것을 확인하고 상기 절차들을 수행하여 해당 Service Request 메시지가 적정한 요청인지 확인할 수 있다.

[0168] NF Producer_2(403)는 NF Consumer_2(402)의 Service 요청이 적정한 요청인 경우 722단계 및 723단계와 같이 해당 Service Request 메시지에 대한 승인을 회신할 수 있다.

[0169] 이때, NF Producer_2(403)는 상기 통지 서비스 가입이 성공한 경우, 해당 UE에 대한 이벤트 발생 시, Response URI로 통지 서비스를 제공해 주기 위해서, 요청 받은 UE의 정보와 해당되는 Event ID, 그리고 Response URI를 저장할 수 있다.

[0170] 만일 상기 언급된 NF Consumer_2(402)의 서비스 요청이 토큰 확인 오류, CCA 인증서 확인 오류, 또는 해당 이벤트의 서비스 제공 등이 불가능한 경우 등의 여러 경우로 해당 요청이 승인할 수 없는 경우, NF Producer_2(403)는 해당 요청을 거절할 수 있다.

[0171] NF Producer_2(403)에서의 Service Response 메시지는 722단계와 같이 SCP(114)를 거쳐 723단계를 통해 NF Consumer_2(402)로 제공되거나 또는, 직접 NF Consumer_2(402)에게 전송(도 7에 예시하지 않음)될 수 있다.

[0172] 성공적인 Service Response 메시지를 수신한 NF Consumer_2(NF Producer_1과 동일한 NF)(402)는 NF Consumer_1(401)의 Service Request 메시지에 대응하여 725단계와 같이 NF Consumer_1(401)로 서비스 응답 메시지를 회신할 수 있다.

[0173] 본 개시의 다른 실시 예로 NF Producer_1(402)은 NF Consumer_1(401)에서의 Service Request 메시지를 수신하고 NF Consumer_1(401)의 권한 검증을 성공한 후, NF Producer_2(403)와 주고 받는 Service Request 메시지와 상관없이 NF Consumer_1(401)에게 Service Response 메시지를 회신할 수 있다.

[0174] NF Producer_2(403)는 요청받은 UE에 대한 상기 요청받은 Event가 발생 시, 726단계 및 727단계와 같이 저장해 두었던 Response URI를 활용하여 NF Consumer_1(401)에게 통지 서비스를 제공할 수 있다. 이때, 통지 서비스는 NF Consumer_1(401)에게 직접 전송(도 7에 예시하지 않음)되거나, 726단계 및 727단계와 같이 SCP(114)를 통해서 전송될 수 있다.

[0175] 도 8은 본 개시의 다양한 실시예에 따른 네트워크 기능(NF) 장치의 블록 구성도이다.

[0176] 도 8을 참조하면, 네트워크 인터페이스(810), NF 제어부(820), NF 메모리 (830)를 포함할 수 있다. 네트워크 인터페이스(810)는 다른 NF와 통신을 위한 인터페이스를 제공할 수 있다. 예컨대, NF가 AMF(120)인 경우 SMF(13

0)과 통신하기 위한 인터페이스를 제공할 수 있다. 다른 예로, NF가 UPF(110)인 경우 RNA(20) 및/또는 AMP(120) 및/또는 DN(180)과 각종 데이터/신호/메시지의 송수신을 위한 인터페이스를 제공할 수 있다.

[0177] NF 제어부(820)는 해당하는 NF의 동작을 제어할 수 있다. 예컨대, NF 제어부(820)는 앞서 설명한 도 2 내지 도 7의 각 NR들의 동작에 대응한 제어를 수행할 수 있다. 또한 이하에서 설명되는 도 9 및 도 10에 대응하는 동작의 제어를 수행할 수 있다. 예컨대, NF가 NRF(117)인 경우 NRF(117)의 동작의 제어를 수행할 수도 있고, NF가 NEF(116)인 경우 NEF(116)의 동작의 제어를 수행할 수도 있으며, NF가 SCP(114)인 경우 그에 따른 동작의 제어를 수행할 수 있다. 또한 NF가 NF Consumer_1(401)인 경우 도 4 내지 도 7에서 설명된 NF Consumer_1(401)의 동작을 수행할 수 있고, NF가 NF Consumer_2이면서 동시에 NF Producer_1(402)인 경우 도 4 내지 도 7에서 설명된 NF Consumer_2 및 NF Producer_1의 동작에 대한 제어를 수행할 수 있다. 동일하게, NF Producer_2(403)인 경우 도 4 내지 도 7에서 설명된 NF Producer_2(403)의 동작에 대한 제어를 수행할 수 있다. 다른 예로, NF가 NF Consumer(901)인 경우 도 9 및 도 10에서 설명하는 NF Consumer(901)의 동작에 대한 제어를 수행할 수 있다. 또한 NF가 NF Producer(902)인 경우에도 도 9 및 도 10에서 설명하는 NF Producer(902)의 동작에 대한 제어를 수행할 수 있다.

[0178] NF 메모리(830)는 NF의 제어를 위한 정보와 제어 중에 발생된 정보 및 본 개시에 따라 필요한 정보들을 저장할 수 있다. 특히 위에서 설명한 바와 같이 NF Consumer로서 동작하기 위한 제어 정보와 NF Producer로서 동작하기 위한 제어 정보를 저장할 수 있다. 또한 NF 메모리(830)는 특정한 UE로 서비스를 제공하기 위해 위에서 설명된 정보들을 저장할 수 있다.

[0179] 도 9는 본 개시의 실시 예에 따른 네트워크 장치 간 REQUEST-RESPONSE 모델의 서비스 요청 및 회신의 인증 및 권한 허가 절차에 따른 신호 흐름도이다.

[0180] 도 9를 참조하여 설명하기에 앞서 본 개시에서 사용되는 네트워크 기능들을 살펴보기로 한다. 먼저 NF Consumer는 NFc(901)로 예시하였으며, NF Producer는 NFp(902)로 예시하였다. 따라서 이하의 설명에서 NF Consumer와 NFc가 혼용되어 사용될 수 있으며, NF Producer와 NFp가 혼용되어 사용될 수 있다. 또한 도 1에서 설명한 SCP(114)와 NRF(117)의 구성 요소들을 이용하는 경우를 가정한다.

[0181] 본 개시의 실시 예에 따라서 NF Consumer는 NF Producer에게 특정 UE(10) 또는 UE의 그룹 등을 대상으로 하는 특정 서비스를 요청하고, 이에 대한 회신을 수신할 수 있다. NF Consumer는 서비스 회신을 수신할 때, 이 서비스 회신을 전송한 NF가 NF Consumer가 서비스를 받고자 예상했던 NF Producer인지 또는 서비스를 받고자 예상했던 NF Producer와 같은 NF Set에 포함된 NF인지 검증할 수 있다. 여기서 NF set은 둘 이상의 NF들을 포함할 수 있으며, 서로 다른 NF가 동일한 서비스를 제공할 수도 있고, 서로 다른 서비스를 제공하는 NF일 수도 있다.

[0182] NF Consumer(901)는 다른 NF에게서 서비스를 받아야 함을 결정하고, 910단계에서 이를 제공해줄 수 있는 NF의 정보를 획득하기 위해 NRF(117)로 NF Discovery Request 메시지를 전송할 수 있다. 이때, NF Discovery Request 메시지는 NF Consumer(901)가 요청하고자 하는 서비스(requested Service Name)과 이를 제공해 줄 NF의 NF type의 정보를 포함하여, NRF(117)에게 요청할 수 있다.

[0183] NF Discovery Request 메시지를 수신한 NRF(117)는 Discovery Request 메시지에서 요청되는 서비스와 NF type을 확인하고 912단계에서 해당 서비스를 제공해 줄 수 있는 NF들의 정보를 포함하는 NF Discovery Response 메시지를 NFc(901)에게 전송할 수 있다. 이때, NF Discovery Response 메시지에 포함되는 서비스를 제공해 줄 수 있는 NF(들)의 정보는 해당 NF instance를 지칭할 수 있는 NF instance ID와 이들 NF instance들의 주소 정보(예를 들어 FQDN 또는 IP 주소 등)를 포함할 수 있다. 또한, 해당 NF instance들이 속한 NF Set을 지칭할 수 있는 NF Set ID 정보를 포함할 수 있다. 본 개시에서 NF instance를 예로서 설명하였으나, 반드시 NF instance일 필요는 없다. 예컨대, NF가 instance로 구현되지 않고 하나의 서버 자체가 NF로 구현되는 경우 서버에 대한 서버 ID와 주소 정보(예를 들어 FQDN 또는 IP 주소 등)를 제공할 수 있다. 즉, NF instance는 NF 서버로 대체 가능하며, 하나의 NF 서버 및/또는 하나의 NF instance는 하나의 독립된 네트워크 엔티티(entity)가 될 수 있다. 이하에서는 설명의 편의를 위해 NF가 instance로 구현된 경우를 가정하여 설명하기로 한다.

[0184] NF Consumer(901)는 914단계에서 NF Discovery Response 메시지에 포함된 NF instance(들)의 정보 및/또는 NF Set의 정보를 각각 후보 NF 인스턴스 리스트(list of candidate NF instances)와 타겟 NF Set의 정보로 저장할 수 있다. 이처럼 저장된 정보는 향후, 이 정보에 대응하여 수신할 Service Response 메시지가 올바른 NF Producer에서 온 것인지 검증할 때 활용할 수 있다.

[0185] NFc(901)는 916단계에서 Service Request 메시지를 전송할 수 있도록 NRF(117)에게서 권한 확인을 수행하고 토

큰을 발행 받기 위하여 Access Token Request 메시지를 전송할 수 있다. 이때, Access Token Request 메시지는 아래의 정보들을 전부 또는 일부 포함할 수 있다.

[0186] - NF Consumer의 NF Instance ID, NF Type

[0187] - 접근 허가를 원하는 NF 서비스에 대한 정보

[0188] - 접근 허가를 원하는 NF Producer(902)의 NF Type 및 NF Producer Instance ID 등의 정보

[0189] 상기 Access Token Request 메시지의 정보는 912단계에서 NF Discovery Response 메시지의 수신 시에 획득한 에서 획득한 NF Instance ID(들)의 정보를 활용하여 NF Producer Instance ID 등의 정보를 지정할 수 있다.

[0190] NRF(117)는 916단계에서 수신된 Access Token Request 메시지에 포함된 정보 및 예상되는 NF Producer가 지정한 정보(예를 들어, 서비스를 받을 수 있는 NF Consumer의 NF type 등)를 활용하여 해당 토큰 요청에 대한 권한 허가를 결정하고 918단계에서 토큰을 발행할 수 있다. 이처럼 발행된 토큰을 포함하는 Access Token Response 메시지는 918단계와 같이 NFR(117)로부터 NFc(901)로 전송될 수 있다.

[0191] 본 개시의 다른 실시 예로 Access Token Request 메시지의 전송 및 Access token Response 메시지의 수신 절차는 NF Discovery Request 메시지 전송 전에 이루어 질 수도 있다.

[0192] NF Consumer(901)는 918단계에서 Access Token Response 메시지를 수신하고, 920단계에서 NFc(901)에 대한 CCA 인증서를 생성할 수 있다.

[0193] NF Consumer(901)는 920단계에서 CCA 인증서를 생성한 후 922단계에서 NF Producer(902)에게 보낼 Service Request 메시지를 SCP(114)에게 전송할 수 있다. 이때, Service Request 메시지는 요청되는 서비스의 정보, CCA 인증서 및 NRF(117)로부터 수신된 토큰을 포함할 수 있다.

[0194] SCP(114)는 922단계에서 수신된 Service Request 메시지에 기빈하여 924단계에서 NFp를 선택할 수 있다. 이후 926단계에서 SCP(114)는 924단계에서 선택한 NFp로 NF Consumer(901)로부터 수신한 Service Request 메시지를 전송할 수 있다. 이때, SCP(114)는 NF Consumer(901)에게서 수신한 Service Request 메시지에 지칭된 NF Producer를 확인할 수 없거나, NF Producer에게 연결이 되지 않는 등의 문제로 NF Producer가 Service Request를 처리할 수 없을 것으로 예상되는 경우, 상기 Service Request를 처리해 줄 다른 후보 NF Producer를 찾고, 찾아진 후보 NF Producer에게 926단계와 같이 Service Request 메시지를 전송할 수 있다.

[0195] 이처럼 다른 NF Producer를 찾는 경우, SCP(114)는 NF Consumer(901)가 요청한 NF Producer와 동일한 NF Set에 속한 NF Instance에서 후보 NF Producer를 찾아야 한다.

[0196] 928단계에서 NF Producer(902)는 926단계에서 수신한 Service Request 메시지에 포함된 토큰과 CCA 인증서를 검증하여 Service Request 메시지를 전송한 NF Consumer(901)를 인증하고 NRF에서 접근 허가를 받은 NF인지 확인할 수 있다. 본 개시에서는 정상적인 경우 즉, Service Request 메시지를 전송한 NF Consumer(901)가 NRF에서 접근 허가를 받은 NF인 경우를 가정한다.

[0197] 이후 NFp(902)는 930단계에서 NFp의 CCA 인증서를 생성할 수 있다.

[0198] NF Producer(902)는 NF Consumer(901)에게 요청받은 Service를 제공하기 위해 NF Consumer(901)에게 Service Response 메시지를 SCP를 경유하여 전송할 수 있다(932, 934). 이때, NF Producer(902)는 NF Consumer(901)에게 930단계에서 자신을 인증할 수 있도록 생성한 CCA 인증서를 Service Response 메시지에 추가하여 전송할 수 있다.

[0199] 본 개시의 실시 예에서 NF Producer(902)가 생성하는 CCA는 NF Consumer(910)의 NF Instance ID, NF Producer(902)의 NF Instance ID, 인증서의 유효기간을 알릴 수 있는 시간 정보, 그리고 NF Producer의 디지털 인증서 또는 디지털 인증서의 URL 정보 등을 포함할 수 있다. NF의 CCA는 NF의 서명 키로 서명될 수 있다.

[0200] SCP(114)는 932단계에서 NFp(902)로부터 수신한 Service Response 메시지를 934단계에서 NFc(901)로 전송할 수 있다.

[0201] NFc(901)는 Service Response 메시지를 수신한 후, 936단계에서 NF Producer(902)의 CCA 인증서를 검증하여 NF Producer(902)를 인증할 수 있다. 또한 이러한 인증 시에, NF Producer(902)가 Service Request 메시지에서 전송한 후보 NF 인스턴스 리스트 또는 타겟 NF Set에 포함되는지 검증할 수 있다. 검증 결과 NF Producer(902)가 Service Request 메시지에서 전송한 후보 NF 인스턴스 리스트 또는 타겟 NF Set에 포함된 경우, 올바른 NF

Producer가 전송한 Service Response 메시지인지 인증할 수 있다.

[0202] 본 개시의 다른 실시 예로, NF Producer(902)가 생성하는 CCA(CCA of NFp)는 NF Producer(902)가 수신한 Service Request 메시지를 전송해준 SCP(114)를 지칭할 수 있는 정보 예를 들어, SCP(114)의 NF Instance ID 등의 정보를 포함할 수 있다.

[0203] NF Producer(902)가 생성하는 CCA(CCA of NFp)를 포함하는 Service Response 메시지를 수신하는 SCP(114)는 2가지 상황을 고려할 수 있다.

[0204] 첫 번째 경우로, SCP(114)가 수신한 Service response 메시지에 포함된 NF Producer(902)가 생성한 CCA(CCA of NFp) 정보에서 지시하는 SCP(114)가 자신인 경우이다. 이런 경우라면, CSP(114)는 자신을 지칭하고 있으므로, 수신한 Service Request 메시지가 정상적인 것으로 인증할 수 있다.

[0205] 두 번째 경우로, SCP(114)가 수신한 Service response 메시지에 포함된 NF Producer(902)가 생성한 CCA(CCA of NFp) 정보에서 지시하는 SCP가 자신이 아닌 다른 SCP(SCP_2)인 경우가 될 수 있다. 이때 단순한 방법은 Service Request 메시지가 비정상적인 것으로 판정(식별)할 수 있다. 하지만, SCP(114)가 수신한 Service response 메시지에 포함된 NF Producer(902)가 생성한 CCA(CCA of NFp) 정보에서 지시하는 SCP가 자신이 아닌 다른 SCP(SCP_2)인 경우에도 정상적인 경우가 포함될 수 있다.

[0206] 가령, Service Request 메시지의 전송을 요청 받은 SCP(SCP_2)가 직접 NF Producer(902)에게 전송하지 않고, 다른 SCP(SCP_1)에게 Service Request 메시지의 전송을 전달하는 경우가 될 수 있다. 이처럼 SCP(SCP_2)가 직접 NF Producer(902)에게 전송하지 않고, 다른 SCP(SCP_1)에게 Service Request 메시지의 전송을 전달하는 경우는 NF Producer(902)가 SCP(SCP_2)의 영역 내에 위치하지 않거나 기타 다른 이유 등이 될 수 있다.

[0207] 이런 경우 Service response 메시지에 포함된 NF Producer(902)가 생성한 CCA(CCA of NFp) 정보에서 지시하는 SCP가 SCP_2를 지시할 수 있다. 그러면, SCP_1은 해당하는 Service Request 메시지에 대하여 SCP_2로부터 전송을 요청 받았는지 여부를 식별하고, 만일 SCP_2로부터 해당하는 Service Request 메시지의 전송을 요청 받은 경우라면, 추가적인 정보를 이용하여 올바른 메시지인지 식별할 수 있다.

[0208] 추가적인 정보를 예를 들면, NF Consumer(901)가 NF Producer(902)로 Service Request 메시지를 전송하고, 해당하는 NF Producer(902)로부터 NF Consumer(901)로 전송되는 응답으로 수신된 것인지를 검증함으로써 올바른 메시지인지 식별(검증)할 수 있다.

[0209] 만일 위의 절차들 중 적어도 하나의 검증에 실패하는 경우 Service Response 메시지를 거절하거나 NFc(901)로 해당하는 Service Response 메시지가 올바른 NF Producer에게서 수신되지 않은 것임을 알릴 수 있다.

[0210] NF Consumer는 SCP로부터 Service Response가 올바른 NF Producer로부터 수신되지 않은 것임을 통지(연락)받는 경우 해당 Service Response가 올바르지 않은 Service Response로 판정하고, 이후 필요한 일련의 동작을 수행할 수 있다.

[0211] 도 10은 본 개시의 실시 예에 따른 네트워크 장치 집합 내의 네트워크 장치 선택을 활용한 네트워크 장치 간 REQUEST-RESPONSE 모델의 서비스 요청 및 회신의 인증 및 권한 허가 절차에 대한 예시도이다.

[0212] 도 10를 참조하여 설명하기에 앞서 본 개시에서 사용되는 네트워크 기능들을 살펴보기로 한다. 먼저 NF Consumer는 도 9에서와 같이 NFc(901)로 예시하였으며, NF Producer는 NFp(902)로 예시하였다. 또한 도 1에서 설명한 SCP(114)와 NRF(117)의 구성 요소들을 이용하는 경우를 가정한다.

[0213] 본 개시의 실시 예에 따라서 NF Consumer(901)는 NF Producer(902)에게 특정 UE 또는 UE의 그룹 등을 대상으로 하는 특정 서비스를 요청하고 이에 대한 회신을 수신할 수 있다. NF Consumer(901)는 서비스 회신을 수신할 때, 이 서비스 회신을 전송한 NF가 NF Consumer(901)가 서비스를 받고자 예상했던 NF Producer(902)인지 또는 서비스를 받고자 예상했던 NF Producer(902)와 같은 NF Set에 포함된 NF 인지 검증할 수 있다. 여기서 NF set은 둘 이상의 NF들을 포함할 수 있으며, 서로 다른 NF가 동일한 서비스를 제공할 수도 있고, 서로 다른 서비스를 제공하는 NF일 수도 있다.

[0214] NF Consumer(901)는 다른 NF에게서 서비스를 받아야 함을 결정하고, 1010단계에서 이를 제공해줄 수 있는 NF의 정보를 획득하기 위해 NRF(117)로 NF Discovery Request 메시지를 전송할 수 있다. 이때, NF Discovery Request 메시지는 NF Consumer(901)가 요청하고자 하는 서비스(requested Service Name)과 이를 제공 해 줄 NF의 NF type의 정보를 포함하여, NRF(117)에게 요청할 수 있다.

[0215] NF Discovery Request 메시지를 수신한 NRF(117)는 NF Discovery Request 메시지에서 요청되는 서비스와 NF type을 확인하고 1012단계에서 해당 서비스를 제공해 줄 수 있는 NF들의 정보를 포함하는 NF Discovery Response 메시지를 NFc(901)에게 전송할 수 있다. 이때, NF Discovery Response 메시지에 포함되는 서비스를 제공해 줄 수 있는 NF(들)의 정보는 해당 NF instance를 지칭할 수 있는 NF instance ID와 이들 NF instance들의 주소 정보(예를 들어 FQDN 또는 IP 주소 등)를 포함할 수 있다. 또한, 해당 NF instance들이 속한 NF Set을 지칭할 수 있는 NF Set ID 정보를 포함할 수 있다. 본 개시에서 NF instance를 예로서 설명하였으나, 반드시 NF instance일 필요는 없다. 예컨대, NF가 instance로 구현되지 않고 하나의 서버 자체가 NF로 구현되는 경우 서버에 대한 서버 ID와 주소 정보(예를 들어 FQDN 또는 IP 주소 등)를 제공할 수 있다. 즉, NF instance는 NF 서버로 대체 가능하며, 하나의 NF 서버 및/또는 하나의 NF instance는 하나의 독립된 네트워크 엔티티(entity)가 될 수 있다. 이하에서는 설명의 편의를 위해 NF가 instance로 구현된 경우를 가정하여 설명하기로 한다.

[0216] NF Consumer(901)는 1014단계에서 NF Discovery Response 메시지에 포함된 NF instance(들)의 정보 및/또는 NF Set의 정보를 각각 후보 NF 인스턴스 리스트(list of candidate NF instances)와 타겟 NF Set의 정보로 저장할 수 있다. 이처럼 저장된 정보는 향후, 이 정보에 대응하여 수신할 Service Response 메시지가 올바른 NF Producer에서 온 것인지 검증할 때 활용할 수 있다.

[0217] NFc(901)는 1016단계에서 Service Request 메시지를 전송할 수 있도록 NRF(117)에게서 권한 확인을 수행하고 토큰을 발행 받기 위하여 Access Token Request 메시지를 전송할 수 있다. 이때, Access Token Request 메시지는 아래의 정보들을 전부 또는 일부 포함할 수 있다.

[0218] - NF Consumer의 NF Instance ID, NF Type

[0219] - 접근 허가를 원하는 NF 서비스에 대한 정보

[0220] - 접근 허가를 원하는 NF Producer(902)의 NF Type 및 NF Producer Instance ID 등의 정보

[0221] 상기 Access Token Request 메시지의 정보는 1012단계에서 NF Discovery Response 메시지에서 획득한 NF Instance ID들의 정보를 활용하여 NF Producer Instance ID 등의 정보를 지정할 수 있다.

[0222] NRF(117)는 Access Token Request 메시지에 포함된 정보 및 예상되는 NF Producer가 지정한 정보(예를 들어, 서비스를 받을 수 있는 NF Consumer의 NF type 등)를 활용하여 해당 토큰 요청에 대한 권한 허가를 결정하고, 1018단계에서 토큰을 발행할 수 있다. 이처럼 발행된 토큰을 포함하는 Access Token Response 메시지로 1018단계와 같이 NFR(117)로부터 NFc(901)로 전송될 수 있다.

[0223] 본 개시의 다른 실시 예로 Access Token Request 메시지의 전송 및 Access token Response 메시지의 수신 절차는 NF Discovery Request 메시지 전송 전에 이루어 질 수도 있다.

[0224] NF Consumer(901)는 1018단계에서 Access Token Response 메시지를 수신하고, 1020단계에서 NFc(901)에 대한 CCA 인증서를 생성할 수 있다.

[0225] NF Consumer(901)는 1020단계에서 CCA 인증서를 생성한 후 1022단계에서 NF Producer(902)에게 보낼 Service Request 메시지를 SCP(114)에게 전송할 수 있다. 이때, Service Request 메시지는 요청되는 서비스의 정보, CCA 인증서 및 NRF(117)로부터 수신한 토큰을 포함할 수 있다. 이때, NF Consumer(901)는 후보 NF 인스턴스 리스트를 Service Request 메시지에 포함하거나 별도의 메시지를 Service Request 메시지와 함께 SCP(114)로 전달할 수 있다. 이처럼 별도의 메시지를 통해 또는 Service Request 메시지의 별도의 필드를 이용하여 후보 NF 인스턴스 리스트를 전송하는 경우 SCP(114)는 지칭된 NF Producer가 연결되지 않을 때, 후보 NF 인스턴스 리스트에서 다른 NF Instance를 선택하고 선택된 NF Instance로 Service Request 메시지를 전송할 수 있다. 즉, SCP(114)는 1022단계에서 수신된 Service Request 메시지에 기반하여 1024단계에서 NFp를 선택할 수 있다.

[0226] SCP(114)는 NF Consumer(901)로부터 수신한 Service Request 메시지를 NF Producer(902)에게 전송할 수 있다. 이때, SCP(114)는 NF Consumer(901)로부터 수신한 Service Request 메시지에 지칭된 NF Producer를 확인할 수 없거나, NF Producer에게 연결이 되지 않는 등의 문제로 NF Producer가 Service Request 메시지를 처리할 수 없을 것으로 예상되는 경우, 수신한 후보 NF 인스턴스 리스트에서 상기 Service Request 메시지를 처리해 줄 다른 후보 NF Producer를 찾고, 찾아진 후보 NF Producer에게 1026단계와 같이 Service Request 메시지를 전송할 수 있다.

[0227] NF Producer(902)는 1026단계에서 수신한 Service Request 메시지에 포함된 토큰과 CCA 인증서를 검증하여 Service Request 메시지를 전송한 NF Consumer(901)를 인증하고 NRF(117)에서 접근 허가를 받은 NF인지 확인할

수 있다. 본 개시에서는 정상적인 경우 즉, Service Request 메시지를 전송한 NF Consumer(901)가 NRF에서 접근 허가를 받은 NF인 경우를 가정한다.

[0228] 이후 NFp(902)는 1030단계에서 NFp의 CCA 인증서를 생성할 수 있다.

[0229] NF Producer(902)는 NF Consumer(901)에게 요청 받은 Service를 제공하기 위해 NF Consumer(901)에게 Service Response 메시지를 SCP(114)를 경유하여 전송할 수 있다(1032, 1034). 이때, NF Producer(902)는 NF Consumer(901)에게 자신을 인증 할 수 있는 CCA 인증서 즉, 1030단계에서 생성한 인증서를 Service Response 메시지에 추가하여 전송할 수 있다.

[0230] 본 개시의 실시 예에서 NF Producer(902)가 생성하는 CCA는 NF Consumer(901)의 NF Instance ID, NF Producer(902)의 NF Instance ID, 인증서의 유효기간을 알릴 수 있는 시간 정보, 그리고 NF Producer의 디지털 인증서 또는 디지털 인증서의 URL 정보 등을 포함할 수 있다. NF의 CCA는 NF의 서명 키로 서명될 수 있다.

[0231] SCP(114)는 1032단계에서 NFp(902)로부터 수신한 Service Response를 1034단계에서 NFc(901)로 전송할 수 있다.

[0232] NFc(901)는 Service Response 메시지를 수신한 후, 1036단계에서 NF Producer의 CCA 인증서를 검증하여 NF Producer(902)를 인증할 수 있다. 또한 이러한 인증 시에, NF Producer(902)가 Service Request 메시지에서 전송한 후보 NF 인스턴스 리스트 또는 타겟 NF Set에 포함되는지 검증할 수 있다. 검증 결과 NF Producer(902)가 Service Request 메시지에서 전송한 후보 NF 인스턴스 리스트 또는 타겟 NF Set에 포함된 경우, 올바른 NF Producer가 전송한 Service Response 메시지인지 인증할 수 있다.

[0233] 본 개시의 또 다른 실시 예로 NF Producer가 생성하는 CCA는 NF Producer가 수신한 Service Request를 전송해준 SCP를 지칭할 수 있는 정보, 예를 들어 SCP의 NF Instance ID 등의 정보를 포함할 수 있다.

[0234] 본 개시의 다른 실시 예로, NF Producer(902)가 생성하는 CCA(CCA of NFp)는 NF Producer(902)가 수신한 Service Request 메시지를 전송해준 SCP(114)를 지칭할 수 있는 정보 예를 들어, SCP(114)의 NF Instance ID 등의 정보를 포함할 수 있다.

[0235] NF Producer(902)가 생성하는 CCA(CCA of NFp)를 포함하는 Service Response 메시지를 수신하는 SCP(114)는 2가지 상황을 고려할 수 있다.

[0236] 첫 번째 경우로, SCP(114)가 수신한 Service response 메시지에 포함된 NF Producer(902)가 생성한 CCA(CCA of NFp) 정보에서 지시하는 SCP(114)가 자신인 경우이다. 이런 경우라면, CSP(114)는 자신을 지칭하고 있으므로, 수신한 Service Request 메시지가 정상적인 것으로 인증할 수 있다.

[0237] 두 번째 경우로, SCP(114)가 수신한 Service response 메시지에 포함된 NF Producer(902)가 생성한 CCA(CCA of NFp) 정보에서 지시하는 SCP가 자신이 아닌 다른 SCP(SCP_2)인 경우가 될 수 있다. 이때 단순한 방법은 Service Request 메시지가 비정상적인 것으로 판정(식별)할 수 있다. 하지만, SCP(114)가 수신한 Service response 메시지에 포함된 NF Producer(902)가 생성한 CCA(CCA of NFp) 정보에서 지시하는 SCP가 자신이 아닌 다른 SCP(SCP_2)인 경우에도 정상적인 경우가 포함될 수 있다.

[0238] 가령, Service Request 메시지의 전송을 요청 받은 SCP(SCP_2)가 직접 NF Producer(902)에게 전송하지 않고, 다른 SCP(SCP_1)에게 Service Request 메시지의 전송을 전달하는 경우가 될 수 있다. 이처럼 SCP(SCP_2)가 직접 NF Producer(902)에게 전송하지 않고, 다른 SCP(SCP_1)에게 Service Request 메시지의 전송을 전달하는 경우는 NF Producer(902)가 SCP(SCP_2)의 영역 내에 위치하지 않거나 기타 다른 이유 등이 될 수 있다.

[0239] 이런 경우 Service response 메시지에 포함된 NF Producer(902)가 생성한 CCA(CCA of NFp) 정보에서 지시하는 SCP가 SCP_2를 지시할 수 있다. 그러면, SCP_1은 해당하는 Service Request 메시지에 대하여 SCP_2로부터 전송을 요청 받았는지 여부를 식별하고, 만일 SCP_2로부터 해당하는 Service Request 메시지의 전송을 요청 받은 경우라면, 추가적인 정보를 이용하여 올바른 메시지인지 식별할 수 있다.

[0240] 추가적인 정보를 예를 들면, NF Consumer(901)가 NF Producer(902)로 Service Request 메시지를 전송하고, 해당하는 NF Producer(902)로부터 NF Consumer(901)로 전송되는 응답으로 수신된 것인지를 검증함으로써 올바른 메시지인지 식별(검증)할 수 있다.

[0241] 만일 위의 절차들 중 적어도 하나의 검증에 실패하는 경우 Service Response 메시지를 거절하거나 NFc(901)로 해당하는 Service Response 메시지가 올바른 NF Producer에게서 수신되지 않은 것임을 알릴 수 있다.

[0242] NF Consumer는 SCP로부터 Service Response가 올바른 NF Producer로부터 수신되지 않은 것임을 통지(연락)받는 경우 해당 Service Response가 올바르지 않은 Service Response로 판정하고, 이후 필요한 일련의 동작을 수행할 수 있다.

[0243] 본 명세서와 도면에 개시된 실시 예들은 본 개시의 내용을 쉽게 설명하고, 이해를 돕기 위해 특정 예를 제시한 것일 뿐이며, 본 개시의 범위를 한정하고자 하는 것은 아니다. 따라서 본 개시의 범위는 여기에 개시된 실시 예들 이외에도 본 개시의 기술적 사상을 바탕으로 도출되는 모든 변경 또는 변형된 형태가 본 개시의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

[0244] 10: UE 20: (R)AN

110: UPF 111: AUSF

112: AMF 113: SMF

114: SCP 115: MSSF

116: NEF 117: NRF

118: PCF 119: UDM

120: AF 130: DN

210: NF 300: NF service consumer

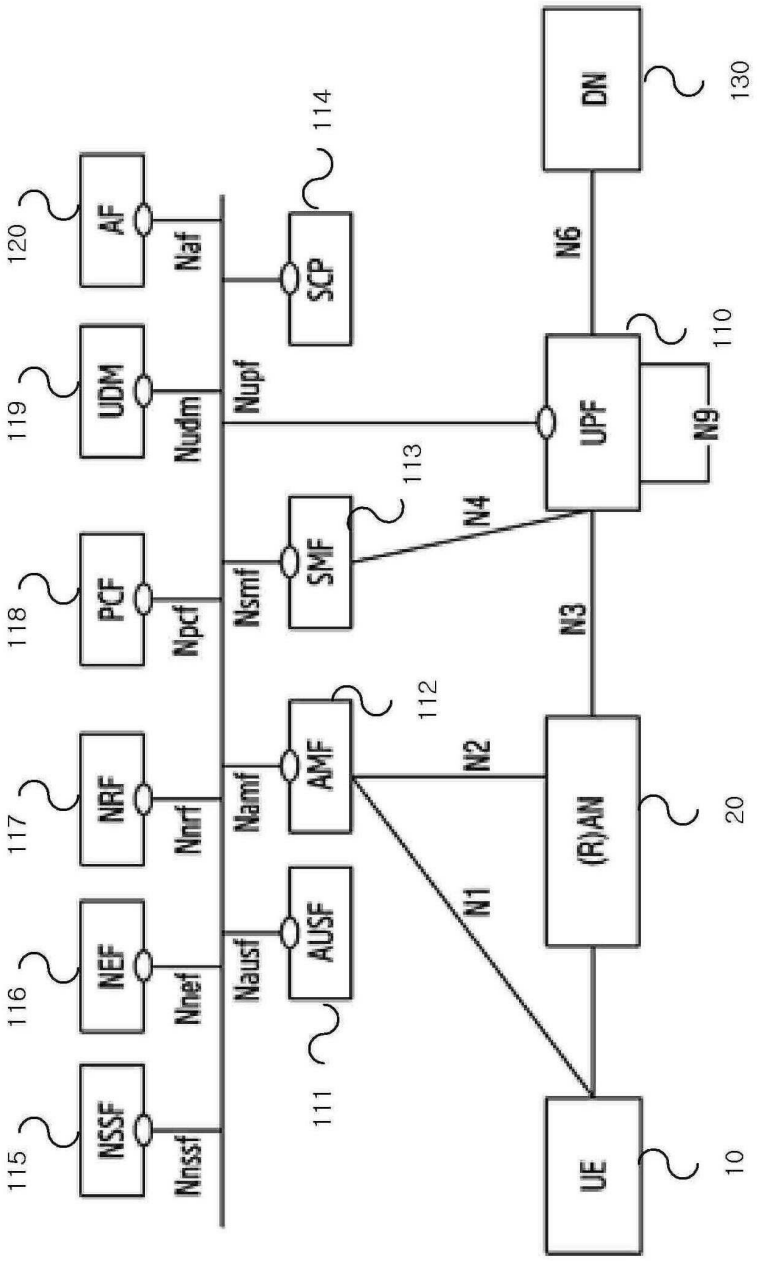
401: NFc_1 402: NFp_1 and NFc_2

403: NFp_2 810: 네트워크 인터페이스

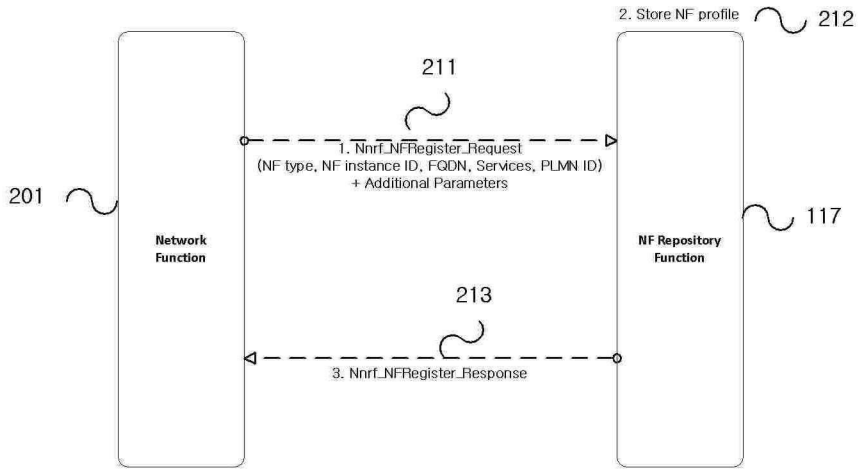
820: NF 제어부 830: NF 메모리

도면

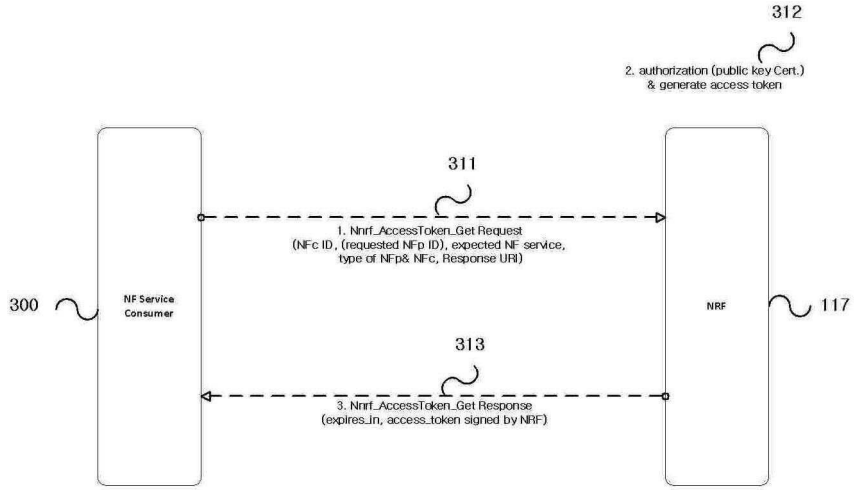
도면1


UE
10
(R)AN
20
AMF
112
SMF
113
AUSF
111
UPF
110
DN
130
SCP
114
AF
120
UDM
119
PCF
118
NRF
117
NEF
116
NSSF
115
N1
N2
N3
N4
N6
N9
Naf
Nudm
Npcf
Nnrf
Nnef
Nnssf
Nupf
Nsmf
Namf
Nausf

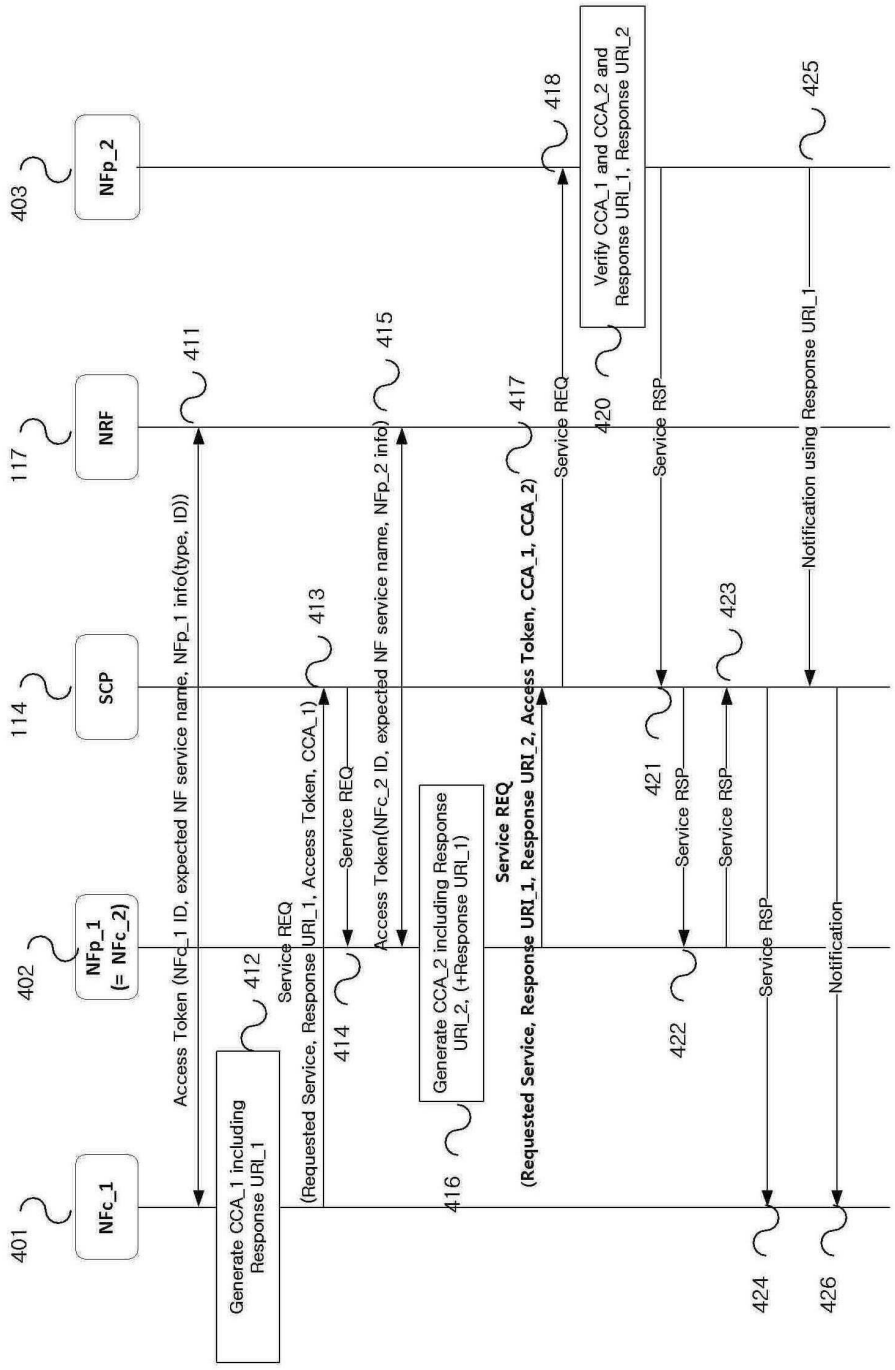
도면2


2. Store NF profile
212
211
1. Nnrf_NFRegister_Request
(NF type, NF instance ID, FQDN, Services, PLMN ID)
+ Additional Parameters
201
Network Function
NF Repository Function
117
213
3. Nnrf_NFRegister_Response

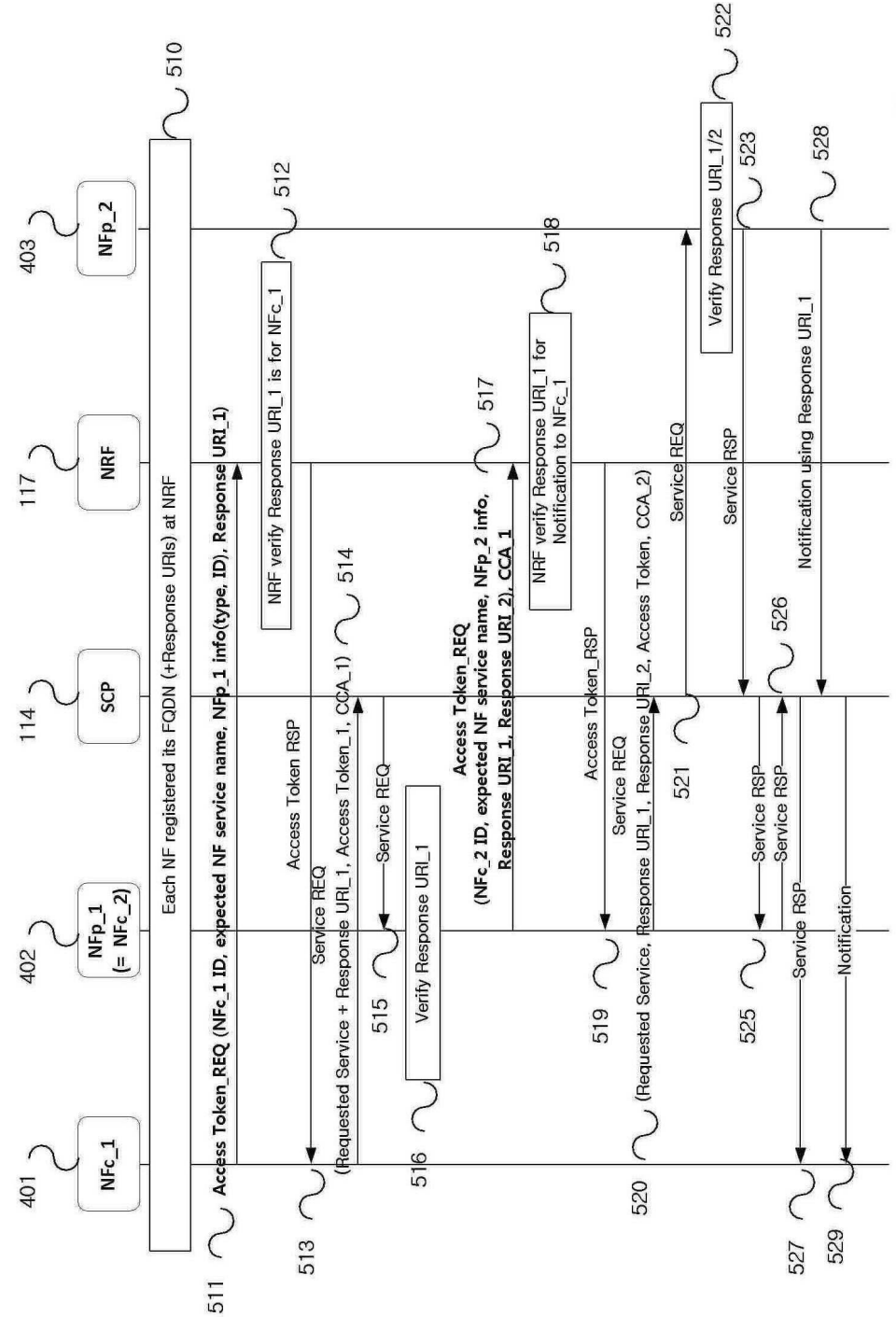
도면3


312
2. authorization (public key Cert.)
& generate access token
311
1. Nnrf_AccessToken_Get Request
(NFc ID, (requested NFp ID), expected NF service,
type of NFp& NFc, Response URI)
300
NF Service Consumer
NRF
117
313
3. Nnrf_AccessToken_Get Response
(expires_in, access_token signed by NRF)

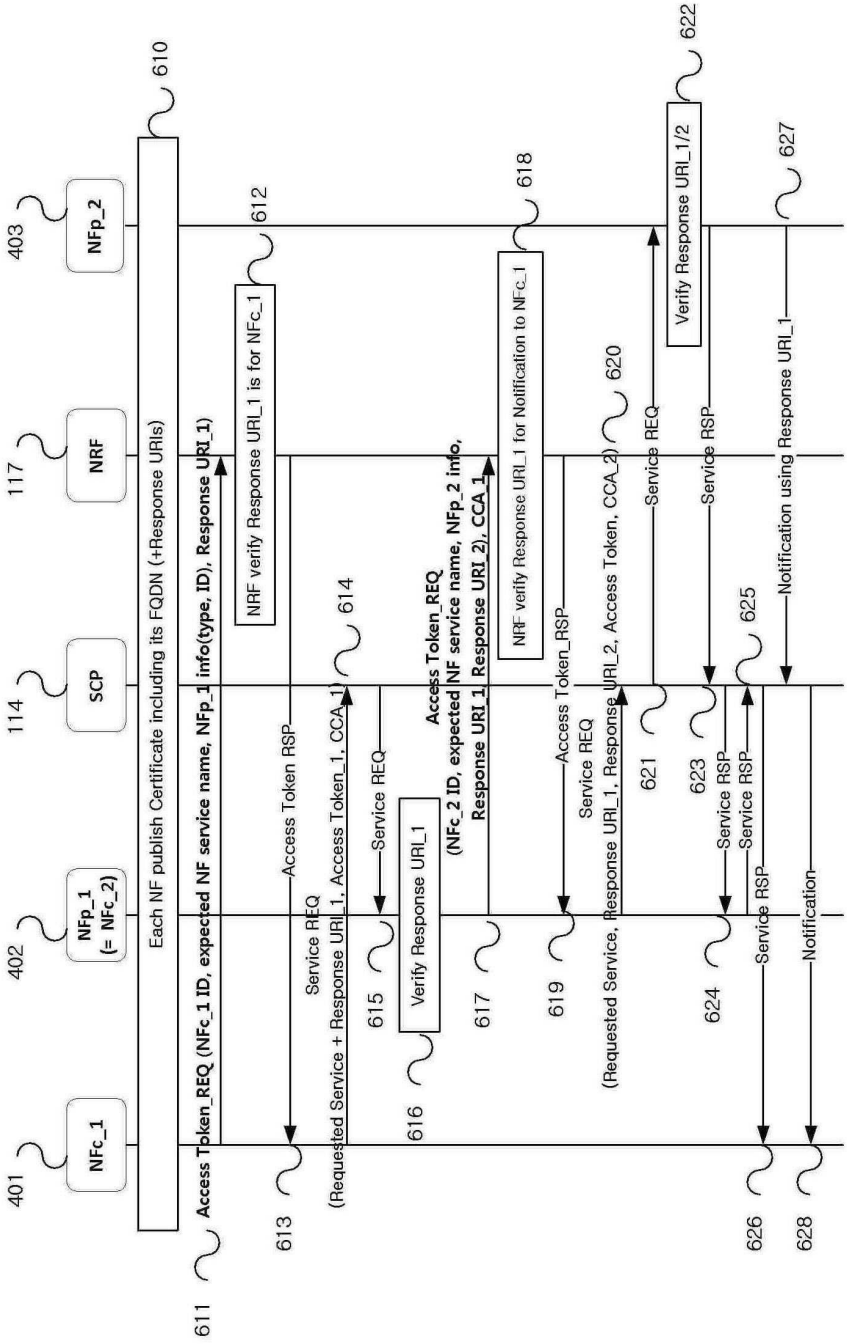
도면4


NFc_1
NFp_1 (= NFc_2)
SCP
NRF
NFp_2
401
402
114
117
403
Access Token (NFc_1 ID, expected NF service name, NFp_1 info(type, ID))
411
Generate CCA_1 including Response URI_1
412
Service REQ (Requested Service, Response URI_1, Access Token, CCA_1)
413
Service REQ
414
Access Token(NFc_2 ID, expected NF service name, NFp_2 info)
415
Generate CCA_2 including Response URI_2, (+Response URI_1)
416
Service REQ (Requested Service, Response URI_1, Response URI_2, Access Token, CCA_1, CCA_2)
417
Service REQ
418
Verify CCA_1 and CCA_2 and Response URI_1, Response URI_2
420
Service RSP
421
Service RSP
422
Service RSP
423
Service RSP
424
Notification using Response URI_1
425
Notification
426

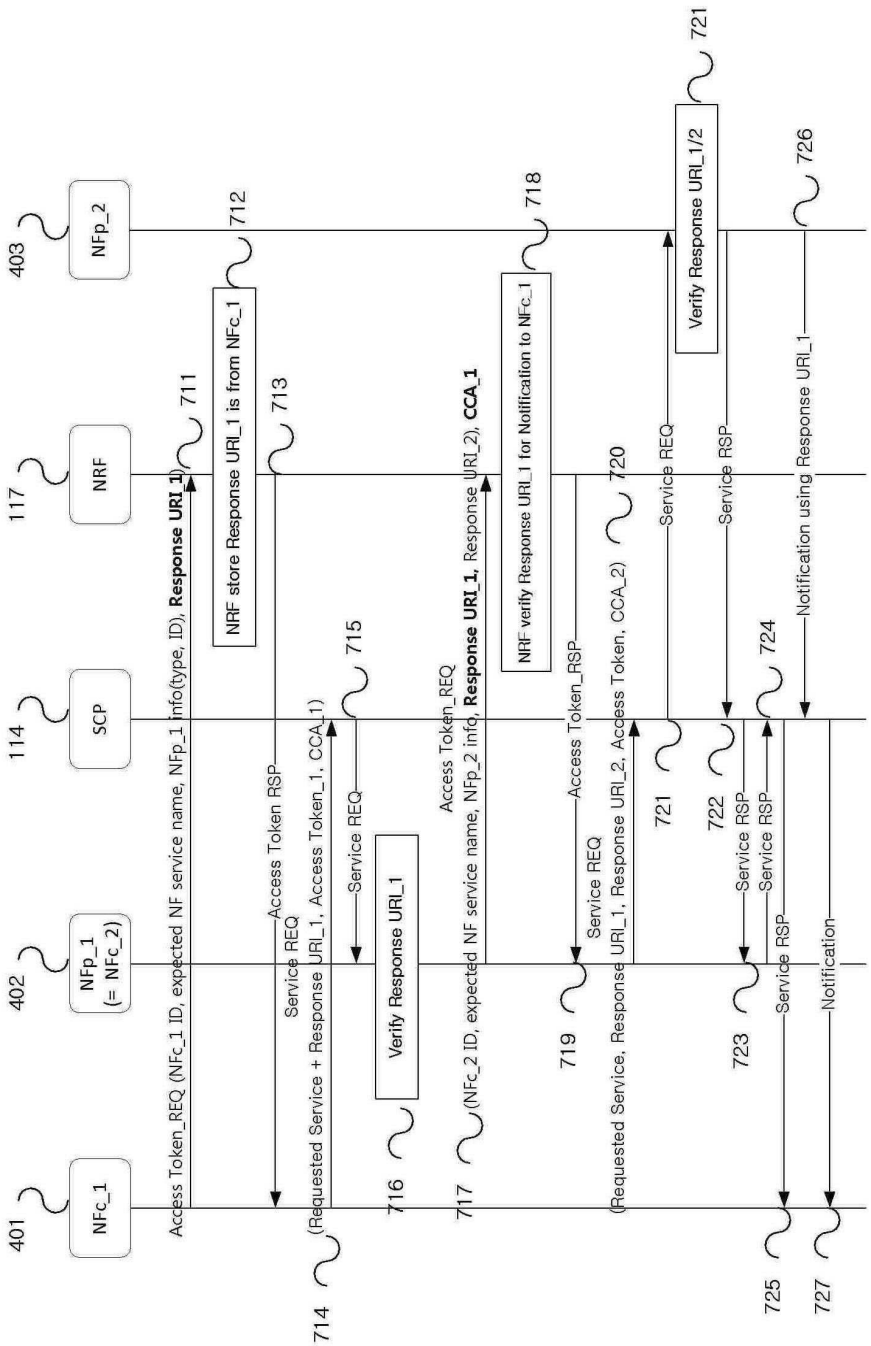
도면5


401
NFc_1
402
NFp_1
(= NFc_2)
114
SCP
117
NRF
403
NFp_2
510
Each NF registered its FQDN (+Response URIs) at NRF
511
Access Token_REQ (NFc_1 ID, expected NF service name, NFp_1 info(type, ID), Response URI_1)
512
NRF verify Response URI_1 is for NFc_1
513
Access Token RSP
Service REQ
(Requested Service + Response URI_1, Access Token_1, CCA_1)
514
Service REQ
515
Verify Response URI_1
516
517
Access Token_REQ
(NFc_2 ID, expected NF service name, NFp_2 info,
Response URI_1, Response URI_2), CCA_1
518
NRF verify Response URI_1 for
Notification to NFc_1
519
Access Token_RSP
Service REQ
520
(Requested Service, Response URI_1, Response URI_2, Access Token, CCA_2)
521
Service REQ
522
Verify Response URI_1/2
523
Service RSP
525
Service RSP
526
Service RSP
527
Service RSP
528
Notification using Response URI_1
529
Notification

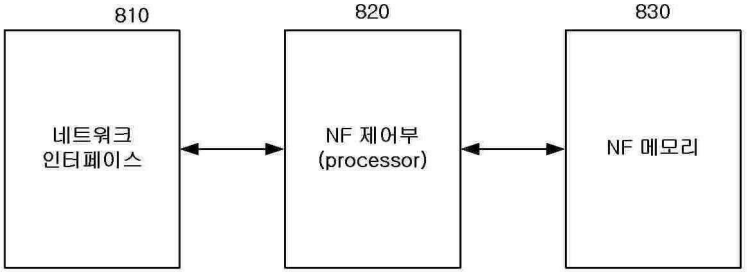
도면6


401
NFc_1
402
NFp_1
(= NFc_2)
114
SCP
117
NRF
403
NFp_2
610
Each NF publish Certificate including its FQDN (+Response URIs)
611
Access Token_REQ (NFc_1 ID, expected NF service name, NFp_1 info(type, ID), Response URI_1)
612
NRF verify Response URI_1 is for NFc_1
613
Access Token RSP
Service REQ
(Requested Service + Response URI_1, Access Token_1, CCA_1)
614
Service REQ
615
Verify Response URI_1
616
Access Token_REQ
(NFc_2 ID, expected NF service name, NFp_2 info,
Response URI_1, Response URI_2), CCA_1
617
618
NRF verify Response URI_1 for Notification to NFc_1
619
Access Token_RSP
Service REQ
(Requested Service, Response URI_1, Response URI_2, Access Token, CCA_2)
620
Service REQ
621
622
Verify Response URI_1/2
623
Service RSP
624
Service RSP
625
Service RSP
626
627
Notification using Response URI_1
628
Notification

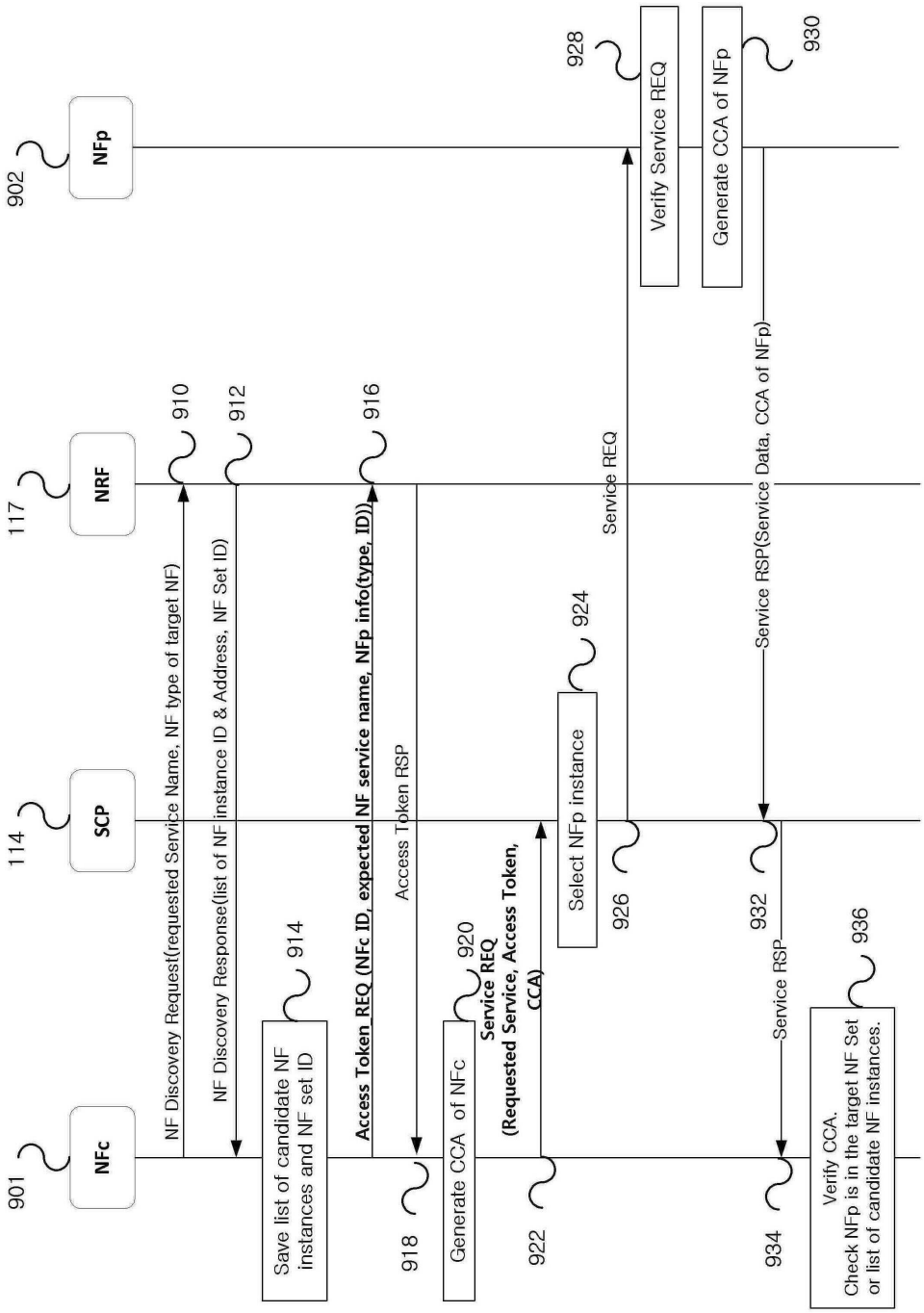
도면7


NFc_1
NFp_1 (= NFc_2)
SCP
NRF
NFp_2
401
402
114
117
403
Access Token_REQ (NFc_1 ID, expected NF service name, NFp_1 info(type, ID), Response URI_1)
711
NRF store Response URI_1 is from NFc_1
712
713
Access Token RSP
Service REQ
(Requested Service + Response URI_1, Access Token_1, CCA_1)
714
Service REQ
715
Verify Response URI_1
716
(NFc_2 ID, expected NF service name, NFp_2 info, Response URI_1, Response URI_2), CCA_1
717
Access Token_REQ
NRF verify Response URI_1 for Notification to NFc_1
718
719
Access Token_RSP
Service REQ
(Requested Service, Response URI_1, Response URI_2, Access Token, CCA_2)
720
721
Service REQ
Verify Response URI_1/2
721
Service RSP
722
Service RSP
723
Service RSP
724
Notification using Response URI_1
726
Service RSP
725
Notification
727

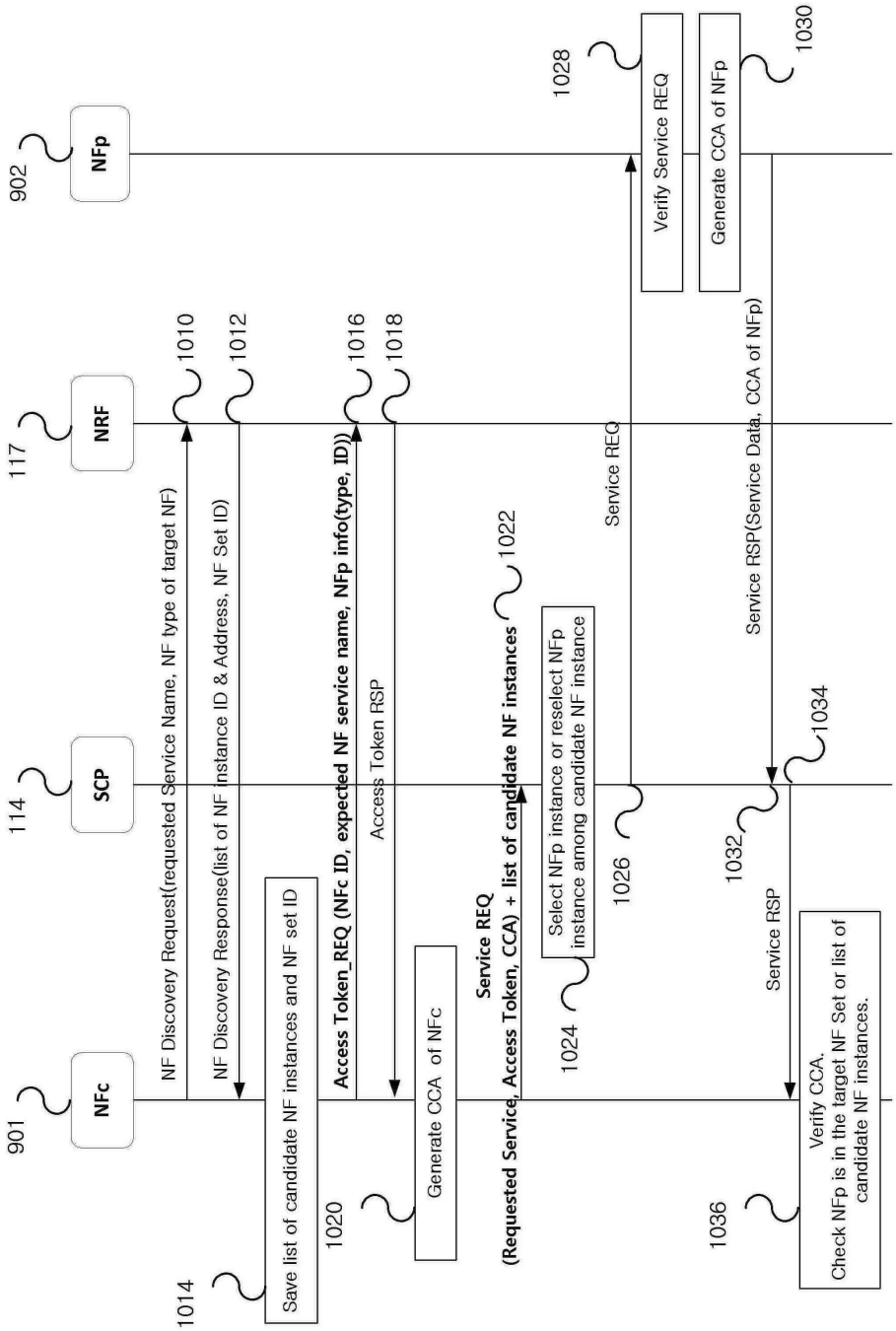
도면8


810
네트워크 인터페이스
820
NF 제어부 (processor)
830
NF 메모리

도면9


NFc
901
SCP
114
NRF
117
NFp
902
NF Discovery Request(requested Service Name, NF type of target NF)
910
NF Discovery Response(list of NF instance ID & Address, NF Set ID)
912
Save list of candidate NF instances and NF set ID
914
Access Token REQ (NFc ID, expected NF service name, NFp info(type, ID))
916
Access Token RSP
Generate CCA of NFc
918
Service REQ (Requested Service, Access Token, CCA)
920
Select NFp instance
922
924
Service REQ
Verify Service REQ
926
928
Generate CCA of NFp
930
Service RSP(Service Data, CCA of NFp)
932
Service RSP
Verify CCA. Check NFp is in the target NF Set or list of candidate NF instances.
934
936

도면10


901
NFc
114
SCP
117
NRF
902
NFp
NF Discovery Request(requested Service Name, NF type of target NF)
1010
NF Discovery Response(list of NF instance ID & Address, NF Set ID)
1012
1014
Save list of candidate NF instances and NF set ID
Access Token_REQ (NFc ID, expected NF service name, NFp info(type, ID))
1016
Access Token RSP
1018
1020
Generate CCA of NFc
Service REQ
(Requested Service, Access Token, CCA) + list of candidate NF instances
1022
1024
Select NFp instance or reselect NFp instance among candidate NF instance
1026
Service REQ
1028
Verify Service REQ
Generate CCA of NFp
1030
Service RSP(Service Data, CCA of NFp)
1032
1034
Service RSP
1036
Verify CCA.
Check NFp is in the target NF Set or list of candidate NF instances.