## 네트워크 권한

네트워크 권한이란 어떤 노드가 특정 노드에 연결하거나 데이터를 전송하는 것을 제어하는 기능입니다. 노드를 기동할 때 --permissioned 플래그를 통해 네트워크 권한 적용이 가능하며, 권한은 각 노드 별로 관리됩니다.

--permissioned 플래그가 설정되면 노드는 *<data-dir>/permissioned-nodes.json* 파일을 찾습니다. 이 파일은 해당 노드가 연결하거나 연결을 허용하는 노드들의 enode 목록입니다. 즉, 네트워크 권한 기능을 사용하면 *permissioned-nodes.json* 파일에 나열된 노드만 네트워크에 참여 가능합니다. --permissioned 플래그를 설정하였지만 *permissioned-nodes.json* 파일에 아무 내용도 기술하지 않는 경우, 이 노드는 다른 어떤 노드와도 연결할 수 없습니다.

*permissioned-nodes.json* 파일은아래와 같이 static-nodes.json 파일(노드가 항상 연결하는 정적(static) 노드 목록)과 비슷한 패턴을 따릅니다.

[ "enode://remoteky1@ip1:port1","enode://remoteky1@ip2:port2","enode://remoteky1@ip3:port3", ]

샘플 파일: (뒷부분 노드 ID 일부 생략)

[ "enode://6598638ac5b15ee386210156a43f565fa8c485924894e2f3a967207c047470@127.0.0.1:30300",]

참고: 현재 버전에서는 모든 노드에 자체의 *permissioned-nodes.json* 파일 사본이 있습니다. 이 경우, 여러 노드가 서로 다른 리모트 키(remote key) 목록을 가지면서 서로 다른 허가된 노드 목록을 가지게 되면(네트워크를 구성하려는 노드들의*permissioned-nodes.json* 파일 내용이 서로 다른 경우) 동작 상에 예상치 못한 문제가 발생할 수 있습니다. 향후에는 허가된 노드 목록을 *permissioned-nodes.json* 파일이 아니라 스마트 컨트랙트로 관리할 것입니다. 이를 통해 네트워크 연결을 확인하려는 모든 노드들은 하나의 글로벌 온 체인(on-chain) 목록을 사용하도록 할 것입니다. 추가로 예정된 개선 사항은 [[제품 로드맵|제품 로드맵]]을 참조하십시오.

## 엔클레이브(Enclave) 암호화 기술

엔클레이브는 xsalsa20poly1305(페이로드 컨테이너에서 사용하는 암호화 모듈) 와 curve25519xsalsa20poly1305(수신자 박스에서 사용하는 비대칭 암호화 모듈)를 사용하는 트랜잭션 매니저를 통해 송신된 페이로드를 암호화합니다. 페이로드 암호화는 각 페이로드별로 암호화를 처리하기 위한 페이로드 컨테이너와 N개의 수신자 박스를 생성하는데, 여기서 N은 트랜잭션의 privateFor 파라미터에 지정된 수신자의 수입니다.   
\*페이로드 컨테이너에는 대칭 키와 임의의 논스(nonce)로 암호화된 페이로드가 들어 있습니다.   
\*수신자 박스는 임의의 논스를 사용하는 수신자의 공개키를 위해 암호화된 페이로드 컨테이너의 마스터 키입니다. (수신자 박스는 기본적으로 PGP(Pretty Good Privacy)가 동작하는 방식과 동일하게 동작하지만 [NaCl](https://nacl.cr.yp.to/) 암호화 라이브러리를 사용한다는 점에 유의하십시오.)

현재 시스템은 퍼블릭 키 목록을 화이트리스트에 수동으로 정의하여야 하고, 키 교체가 자동화 되어있지 않지만 네트워크를 구성하는 노드들에서 여러 키를 한 번에 공고할 수 있도록 하여 기본적인 키 교체 기능을 제공하고 있습니다. 이를 원활하고 자동화할 수 있도록 돕는 툴은 [제품 로드맵|제품 로드맵]]에서 확인하십시오. 또한, Quorum은 현재 PKI 시스템을 가지고 있지 않지만, 화이트리스트에 수동으로 추가될 키를 임의로 생성할 수 있도록 기능을 제공하고 있습니다. (예시: 블록체인에서 허가된 다른 노드의 레지스트리) 이 프로세스는 현재 운영자가 키 쌍을 생성한 다음 수동으로 화이트리스트에 추가하는 것입니다.

## 프라이빗 키 저장 알고리즘

프라이빗 키를 관리하는 방법은 아래와 같습니다. 1. 패스워드 P 부여 2. 임의의 Argon2i 논스 생성 3. 임의의 NaCl 시크릿박스 논스 생성 4. 32바이트 마스터키(MK)에 Argon2i (및 Argon2i nonce)를 사용하여 P 늘림 5. 시크릿박스 논스 및 Argon2로 늘린 마스터키를 이용하여 시크릿박스의 프라이빗 키 암호화