

단말, 펌웨어, eSIM 가이드

Q1. 단말(Device)과 네트워크 사이의 기본 통신 절차는 어떻게 이루어지나요?

A1. 기본 절차는 다음과 같습니다:

1. 전원 On → 기지국 수신 감지
2. 셀 서치(Cell Search) → 강도/품질 기준 셀 선택
3. RRC 연결 요청(RRC Connection Request)
4. Attach/Registration 절차 수행
5. PDN 연결 및 IP 할당

이후 단말은 EPS Bearer 또는 PDU Session을 통해 트래픽을 송수신합니다.

Q2. 단말에서 발생할 수 있는 통신 불량 유형은 무엇인가요?

A2. - Attach 실패: 인증/식별 오류, SIM 불량

- DRX 설정 문제: 데이터 지연, 비정상 절전

- Handover 실패: 무선 파라미터 오류, 타이밍 불일치

- PDN 연결 실패: APN 설정 문제, EPC 오류

이슈 발생 시 UE 로그 + Cell 측 KPI + MME/AMF Log를 종합 분석합니다.

Q3. 단말 로그(Logcat, QXDM 등)를 통해 어떤 정보를 확인할 수 있나요?

A3. - RRC 메시지 흐름

- NAS 단계에서의 오류 코드

- eSIM 상태, 프로파일 여부

- Radio 상태 (RSRP, SINR, Cell ID)

- PLMN 선택, 타이머 동작(T3412 등)

장비와 OSS 상 로그 매칭을 통해 상세 분석이 가능합니다.

Q4. 펌웨어(Firmware) 업데이트는 어떤 방식으로 관리되고 배포되나요?

A4. 1. 제조사에서 펌웨어 이미지 배포

2. FOTA (Firmware Over The Air) 방식으로 배포

3. 기지국 또는 OTA 서버에서 대상 단말 식별

4. 업데이트 완료 후 버전 확인 및 검증

운영사에서는 버전별 호환성, KPI 영향도를 검토하며 FOTA 배포 일정을 결정합니다.

Q5. eSIM과 물리 SIM의 기술적 차이는 무엇인가요?

A5. - eSIM은 단말 내장형 칩(Embedded UICC)

- 원격으로 프로파일을 다운로드/삭제 가능
 - 물리 SIM은 교체가 가능하나 eSIM은 불가
 - eSIM은 GSMA의 RSP(Remote SIM Provisioning) 규격을 따름
- 보안성과 관리 편의성 측면에서 eSIM이 우수합니다.

Q6. eSIM 발급 절차는 어떻게 구성되며 어떤 시스템이 연동되나요?

A6. 1. 고객 요청 (앱 또는 웹 포털)

2. SM-DP+ 서버에서 프로파일 생성

3. QR 코드 또는 Activation Code 전송

4. 단말이 SM-DP+에 연결 → 프로파일 다운로드

5. LPA(Local Profile Assistant)가 설치 및 활성화

이 과정은 BSS, SM-DP+, SM-DS, 인증 서버와 연동됩니다.

Q7. 단말에서 eSIM 프로파일이 설치되지 않는 주요 원인은 무엇인가요?

A7. LPA 앱 미설치 또는 버전 미지원, SM-DP+ 서버 접근 불가 (방화벽, 인증 실패)

QR 코드 만료 또는 형식 오류, 단말 OS 또는 펌웨어 버그, UICC 잠금 상태 (Carrier Lock)

이슈 발생 시 프로파일 로그 확인 및 서버 측 세션 추적이 필요합니다.

Q8. 다중 SIM 단말에서 데이터/음성 우선 순위는 어떻게 설정되나요?

A8.

- 안드로이드 기준: 설정 > 네트워크 > SIM 우선 순위 설정
- 통신사 앱에서도 설정 가능
- 일반적으로 Data SIM 설정이 우선 적용되며, VoLTE/VoNR는 SIM별 설정 필요
- 일부 단말은 자동 전환 기능을 지원하나, 통신망 등록 기준은 설정에 따라 다릅니다.

Q9. eSIM 발급 시스템(SM-DP+, SM-DS)은 어떤 역할을 하나요?

A9. - SM-DP+ (Subscription Manager - Data Preparation +): 프로파일 생성, 다운로드 트리거 관리

- SM-DS (Discovery Server): 단말이 어떤 SM-DP+에 연결할지 알려주는 역할

LPA (단말 앱)는 이 정보로 해당 SM-DP+에 접속하여 프로파일을 다운로드합니다.

Q10. 단말 호환성 확인은 어떻게 진행되나요?

A10.

- IMEI 기반 단말 DB 조회
- 지원 밴드(Band) 정보 확인 (LTE: B1/B3/B8 등, 5G: n78/n28 등)
- eSIM 지원 여부, FOTA 가능 여부 확인
- 자사망에서 인증된 단말 리스트와 비교

이 정보는 내부 인증 시스템 또는 OSS와 연동된 DB에서 관리됩니다.

Q11. 5G 단말에서 SA/NSA 모드는 어떻게 구분되고 설정되나요?

A11.

- NSA (Non-Standalone): LTE와 5G 병행 운용, EN-DC 기반
- SA (Standalone): 5G Core 단독 운용, PDU Session
- 대부분 단말은 자동 모드이나, 개발자 모드나 Field Test Mode에서 확인/설정 가능
- OSS에서 단말 Capability 보고서를 통해 모드 지원 여부를 확인합니다.

Q12. 단말 통신 장애 시 OSS와 어떤 방식으로 연계 분석하나요?

A12.

1. IMSI/IMEI 기반 CDR 또는 Attach 로그 조회
2. RRC/NAS 실패 로그 분석
3. 셀 KPI 확인 (ERAB 성공률, RLF 등)
4. 단말 측 로그와 매칭

통신사 내부 Trouble Ticket 시스템에서 단말 로그와 OSS 로그가 통합 조회됩니다.

Q13. 단말 펌웨어 버전별로 KPI 영향이 발생할 수 있나요?

A13.

예, 다음과 같은 영향이 있습니다: Ping 지연 증가, Handover 실패 증가, VoLTE 통화 중 끊김 (Codec 처리 이슈), 단말 설정값 무시 현상

운영사는 KPI 기반으로 버전별 문제점을 추출하고 제조사에 패치 요청을 진행합니다.

Q14. 단말 인증 시스템은 어떤 기준으로 작동하나요?

A14.

- IMEI/MEID를 기준으로 단말 인증 여부 확인
- OS 버전, VoLTE 인증 여부, Band 지원 여부 등
- 최초 통신 시 인증 절차가 이루어지며, 미인증 단말은 서비스 제한 가능
- 인증 DB는 주기적으로 갱신되며, 비정상 단말은 블랙리스트 처리됩니다.

